

Publication Number: 53-1000435-01
15 June 2007



Web Tools

Administrator's Guide

Supporting Fabric OS v5.3.0

BROCADE

Copyright © 2006-2007, Brocade Communications Systems, Incorporated.

ALL RIGHTS RESERVED.

Brocade, the Brocade B weave logo, Fabric OS, File Lifecycle Manager, MyView, Secure Fabric OS, Brocade, and StorageX are registered trademarks and Tapestry is a trademark of Brocade Communications Systems, Inc., in the United States and/or in other countries. FICON is a registered trademarks of IBM Corporation in the U.S. and other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

Notice: The information in this document is provided "AS IS," without warranty of any kind, including, without limitation, any implied warranty of merchantability, noninfringement or fitness for a particular purpose. Disclosure of information in this material in no way grants a recipient any rights under Brocade's patents, copyrights, trade secrets or other intellectual property rights. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

Notice: The product described by this document may contain "open source" software covered by the GNU General Public License or other open source license agreements. To find-out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

Export of technical data contained in this document may require an export license from the United States Government.

Brocade Communications Systems, Incorporated

Corporate Headquarters

Brocade Communications Systems, Inc.
1745 Technology Drive
San Jose, CA 95110
Tel: 1-408-333-8000
Fax: 1-408-333-8101
Email: info@brocade.com

Asia-Pacific Headquarters

Brocade Communications Singapore Pte. Ltd.
9 Raffles Place
#59-02 Republic Plaza 1
Singapore 048619
Tel: +65-6538-4700
Fax: +65-6538-0302
Email: apac-info@brocade.com

European and Latin American Headquarters

Brocade Communications Switzerland Sàrl
Centre Swissair
Tour A - 2ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 56 40
Fax: +41 22 799 56 41
Email: emea-info@brocade.com

Document History

The following table lists all versions of the *Web Tools Administrator's Guide*.

Document Title	Publication Number	Summary of Changes	Publication Date
<i>Web Tools User's Guide v2.0</i>	53-0001536-01	N/A	September 1999
<i>Web Tools User's Guide v2.2</i>	53-0001558-02	N/A	May 2000
<i>Web Tools User's Guide v2.3</i>	53-0000067-02	N/A	December 2000
<i>Web Tools User's Guide v3.0</i>	53-0000130-03	N/A	July 2001
<i>Web Tools User's Guide v2.6</i>	53-0000197-02	N/A	December 2001
<i>Advanced Web Tools User's Guide v3.0 / v4.0</i>	53-0000185-02	N/A	March 2002
<i>Advanced Web Tools User's Guide v4.0.2</i>	53-0000185-03	N/A	September 2002
<i>Advanced Web Tools User's Guide v3.1.0</i>	53-0000503-02	N/A	April 2003
<i>Advanced Web Tools User's Guide v4.1.0</i>	53-0000522-02	N/A	April 2003
<i>Advanced Web Tools User's Guide v4.1.2</i>	53-0000522-04	Insistent Domain ID Mode. Port Swapping information. Minor editorial changes	October 2003
<i>Advanced Web Tools Administrator's Guide, v4.2.0</i>	53-0000522-05	Updates to support new switch types: Brocade 3250, 3850, 24000. Structural changes, Support changes, Installation changes.	December 2003
<i>Advanced Web Tools User's Guide</i>	53-0000522-06	Clarifications on software and hardware support, minor enhancements in procedure text, minor rearranging of content.	March 2004
<i>Advanced Web Tools Administrator's Guide</i>	53-0000522-07	Updates to support new switch types (3016, 4100) and Fabric OS v4.4.0, including Ports on Demand, user administration, and zoning wizards.	September 2004
<i>Web Tools Administrator's Guide</i>	53-0000522-08	Updates to support new switch types (200E, 48000) and Fabric OS v5.0.1, including switchAdmin role, upfront login, and Web Tools EZ.	April 2005
<i>Web Tools Administrator's Guide</i>	53-0000522-09	Updates to add additional information about refresh and polling rates.	July 2005

Document Title	Publication Number	Summary of Changes	Publication Date
<i>Web Tools Administrator's Guide</i>	53-1000049-01	Updates to support new switch types (4900, 7500) and Fabric OS v5.1.0, including FCR, FCIP, and the FR4-18i port blade. Web Tools EZ information is moved to a separate book.	January 2006
<i>Web Tools Administrator's Guide</i>	53-1000049-02	Updates to the FCIP chapter to clarify how to configure tunnels.	April 2006
<i>Web Tools Administrator's Guide</i>	53-1000194-01	Updates for Fabric OS v5.2.0 and the FC4-16IP blade. Also new security for Web Tools, including Role-Based Access Control and administrative domains.	September 2006
<i>Web Tools Administrator's Guide</i>	53-1000194-01	Updates to reflect interface enhancements, support for new switch types, IPv6 support, and other enhancements.	June 2007

Contents

About This Document

How this document is organized	ix
Supported hardware and software	x
What's new in this document	xi
Document conventions	xii
Text formatting	xii
Notes, cautions, and warnings	xii
Key terms	xii
Additional information	xiii
Brocade resources	xiii
Optional Brocade features	xv
Other industry resources	xvi
Getting technical help	xvi
Document feedback	xvii

Chapter 1

Introducing Web Tools

In this chapter	1
Requirements, installation, and support	1
Requirements	1
Installing a Web Tools license	6
Value line licenses	8
Launching Web Tools	8
Administrative domains	9
Admin domains and login	10
Admin Domains and switch WWN	11
Admin domains and zoning	11
Role-Based access control	11
Session management	12
Logging In	12
Logging out	14
Requirements for IPv6 support	15

Chapter 2

Using the Web Tools Interface

In this chapter	17
Viewing Switch Explorer	17
Tasks	19
Fabric Tree	19
Admin Domain Context	20
Switch View buttons	21
Switch View	21
Switch Events and Switch Information	22
Displaying tool tips	22

Refresh rates	24
Displaying switches in the fabric	24
Using Web Tools and secure mode	25
Web Tools Access and HTTP_POLICY	25
Opening modules in a secure fabric	25
Primary-FCS-only functionality	26
Disabled functionality	26
Working with Web Tools: recommendations	26

Chapter 3

Managing Fabrics and Switches

In this chapter	29
Managing fabrics and switches using Web Tools	29
Opening the Switch Administration window	31
Refreshing the Switch Administration window	31
Opening the telnet window	31
Configuring IP and netmask information	32
Configuring a syslog IP address	33
Filtering IP Addresses	34
Managing blades	34
Enable or disable a blade	35
Configuring a switch	37
Enabling and disabling a switch	37
Changing the Switch Name	37
Changing the Switch Domain ID	38
Viewing and printing a switch report	38
Rebooting the switch	39
Performing a fast boot	39
Performing a reboot	39
Changing system configuration parameters	39
Configuring fabric parameters	39
Enabling insistent domain ID mode	41
Configuring virtual channel settings	42
Configuring arbitrated loop parameters	42
Configuring system services	43
Managing licensed features	43
Activating a license on a switch	44
Removing a license from a switch	45
Administering High Availability	45
Launching the High Availability Module	45
Synchronizing Services on the CP	46
Initiating a CP Failover	47
Monitoring events	48
Displaying Fabric Events	49
Displaying Switch Events	50
Filtering Fabric and Switch Events	51
Displaying a fabric summary report	53
Displaying the Name Server entries	53
Physically locating a switch using beaconing	55

Chapter 4	Maintaining Configurations and Firmware	
	Maintaining configurations.	57
	Backing Up a configuration file.	58
	Restoring a configuration	59
	Performing a firmware download.	60
 Chapter 5	 Managing Your Ports	
	In this chapter	63
	Viewing and managing ports using Web Tools	63
	Port Administration window components.	65
	Identifying controllable ports.	66
	Configuring ports.	67
	Configuring FC ports	67
	Configuring FCIP ports.	69
	Configuring GbE ports	70
	Assigning a name to a port.	70
	Enabling and disabling a port	71
	Persistent enabling and disabling ports	71
	Enabling and disabling NPIV ports.	72
	Activating ports	73
	Swapping port index	75
 Chapter 6	 Administering ISL Trunking	
	In this chapter	77
	About Interswitch Link Trunking.	77
	Displaying trunk group information	78
	Disabling or reenabling trunking mode on a port.	78
 Chapter 7	 Managing Administrative Domains	
	In this chapter	81
	About administrative domains	81
	Requirements for admin domains	81
	User-defined admin domains	82
	System-defined admin domains.	82
	Admin domain membership	83
	Implementing administrative domains	83
	Using the Admin Domain window.	84
	Opening the Admin Domain window.	86
	Refreshing fabric information	87
	Refreshing admin domain information.	87
	Saving local admin domain changes	87
	Closing the Admin Domain window	88
	Creating and populating domains	88
	Managing administrative domains	91
	Adding and removing members	91
	Renaming admin domains	93
	Deleting admin domains	93

Chapter 8

Administering Zoning

In this chapter	95
Introducing zoning.	95
Zoning and admin domains	96
Configuring zoning	96
Opening the Zone Administration window	96
Setting the default zoning mode.	97
Managing zoning with Web Tools.	97
Refreshing fabric iNfOrMation	99
Refreshing Zone Administration window Information	99
Saving local zoning changes	100
Closing the Zone Administration window	101
Zoning views.	101
Managing zone aliases.	102
Creating and populating zone aliases	102
Adding and removing members of a zone alias.	103
Renaming zone aliases	103
Deleting zone aliases.	103
Managing zones	104
Creating and populating zones.	104
Adding and removing members of a zone	105
Renaming zones.	105
Copying zones	106
Deleting zones	106
Managing zone configurations.	106
Creating zone configurations	107
Adding or removing zone configuration members.	108
Renaming zone configurations	108
Copying zone configurations	109
Deleting zone configurations	109
Enabling zone configurations	109
Disabling zone configurations.	110
Displaying enabled zone configurations.	110
Displaying zone configuration summaries.	112
Creating configuration analysis reports	113
Displaying zones Initiator/Target accessibility.	113
Managing the zoning database	114
Adding a WWN to multiple aliases and zones	114
Removing a WWN from multiple aliases and zones	115
Replacing a WWN in Multiple Aliases and Zones	115
Searching for zone members	115
Clearing the Zoning Database.	116
Using Zoning Wizards	116
Best practices for zoning	119

Chapter 9

Monitoring Performance

In this chapter	121
Monitoring performance using Web Tools.	121
Predefined performance graphs.	122
User-defined graphs.	125
Canvas configurations	126

Opening the Performance Monitoring window	126
Creating basic performance monitor graphs	127
Customizing basic monitoring graphs	127
Creating advanced performance monitoring graphs	129
Creating SID-DID Performance Graphs	129
Creating an SCSI vs. IP Traffic Graph	130
Creating SCSI Command Graphs	131
Creating AL_PA Error Graphs	132
Managing performance graphs	132
Saving graphs to a canvas	132
Adding graphs to a canvas	133
Printing graphs	133
Modifying graphs	134

Chapter 10

Using the FC-FC Routing Service

In this chapter	135
Supported switches for fibre channel routing	135
About fibre channel routing	135
McData interoperability	136
Setting up FC-FC routing	137
Managing FC-FC routing with Web Tools	138
Launching the FC Routing module	138
Viewing and managing LSAN fabrics	139
Viewing and configuring EX_Ports	140
Viewing and configuring FCR router port cost	142
Viewing and configuring LSAN zones	142
Viewing LSAN Devices	143
Configuring the backbone fabric ID	144

Chapter 11

Working With Diagnostic Features

In this chapter	147
Managing trace dumps	147
How a trace dump is used	148
Setting up automatic trace dump transfers	148
Disabling automatic trace uploads	149
Displaying switch information	149
Displaying detailed fan hardware status	150
Displaying the temperature status	151
Displaying the power supply status	151
Checking the physical health of a switch	152
Interpreting port LEDs	154
Port icon colors	155
LED representations	155
Brocade 48000 Director LEDs	156

Chapter 12

Administering Fabric Watch

In this chapter	157
Introduction to Fabric Watch	157
Using Fabric Watch with Web Tools	158

	Configuring Fabric Watch thresholds.	159
	Configuring threshold traits.	159
	Configuring threshold alarms	161
	Enabling or disabling threshold alarms for individual elements	161
	Configuring alarms for FRUs.	162
	Displaying Fabric Watch alarm information.	163
	Displaying an alarm configuration Report	163
	Displaying alarms.	163
	Configuring email notifications	164
	Configuring the email server on a switch.	164
	Configuring the email alert recipient	164
Chapter 13	Administering Extended Fabrics	
	In this chapter	167
	About extended link buffer allocation	167
	Configuring a port for long distance	169
Chapter 14	Administering the iSCSI Target Gateway	
	In this chapter	171
	Supported platforms for iSCSI	171
	About the iSCSI service.	171
	Common Functions in the iSCSI Target Gateway Admin module	172
	Terminology	173
	Saving Changes	174
	Setting up iSCSI Target Gateway Services.	174
	Launching the iSCSI Target Gateway Admin Module.	175
	Activating the iSCSI Feature	176
	Configuring the IP Interface	176
	Managing the iSCSI Virtual Targets	179
	Viewing iSCSI Initiators	181
	Managing Discovery Domains.	182
	Configuring CHAP.	185
	Configuring an iSCSI Fibre Channel Zone	187
	Managing and Troubleshooting Accessibility	189
Chapter 15	Using the Access Gateway	
	Enabling Access Gateway mode.	191
	Displaying the port mapping	192
	Configuring port maps	193
	Enabling failover and failback policies	193
	Converting ports	194
Chapter 16	Routing Traffic	
	In this chapter	197
	About routing.	197
	Displaying FSPF routing	198
	Enabling and disabling dynamic load sharing.	199
	Specifying frame order delivery	199
	Configuring link cost	200

Chapter 17	Configuring Standard Security Features
	In this chapter 201
	Creating and maintaining user-defined accounts. 201
	Creating and Deleting User-Defined Accounts. 203
	Changing Account Parameters 205
	Maintaining Passwords 206
	Configuring access control list policies 209
	Configuring SNMP 211
	Setting SNMP Trap Levels 211
	Configuring SNMP Information 212
	Managing RADIUS service 213
	Enabling and Disabling RADIUS Service 215
	Configuring the RADIUS Service 216
	Modifying the RADIUS Server 216
	Modifying the RADIUS Server Order 217
	Removing a RADIUS Server. 217
 Chapter 18	 Administering FICON CUP Fabrics
	In this chapter 219
	About FICON CUP fabrics 219
	Enabling port-based routing on the Brocade 4100, 5000, and 48000 220
	Enabling or disabling FMS mode 221
	Configuring FMS parameters 222
	Displaying code page information 223
	Displaying the control device state 223
	Configuring CUP port connectivity 224
	Displaying CUP Port Connectivity Configurations 225
	Creating or Editing CUP Port Connectivity Configurations. . . 226
	Activating a CUP Port Connectivity Configuration 228
	Copying a CUP Port Connectivity Configuration 228
	Deleting a CUP Port Connectivity Configuration 228
 Chapter 19	 Limitations
	In this chapter 231
	General Web Tools limitations 231
	Platform-specific limitations. 235
 Index	

About This Document

This preface contains the following sections:

• How this document is organized	ix
• Supported hardware and software	x
• What's new in this document	xi
• Document conventions	xii
• Additional information	xiii
• Getting technical help	xvi
• Document feedback	xvii

How this document is organized

This document is organized to help you find the information that you want as quickly and easily as possible. It provides both concepts and procedures. Because this document primarily guides you through administrative tasks in Web Tools, it is arranged in a loosely chronological order, beginning with prerequisites to getting started and ending with troubleshooting information.

Throughout the document the terms GbE and GigE are used interchangeably to refer to 1 Gigabit. The document contains the following topics:

- [Chapter 1, “Introducing Web Tools”](#), provides some basic information about the Web Tools interface, including system requirements and installation instructions.
- [Chapter 2, “Using the Web Tools Interface”](#), describes the components of the Web Tools interface.
- [Chapter 3, “Managing Fabrics and Switches”](#), provides information on how to manage your fabric and switches using the Web Tools interface.
- [Chapter 4, “Maintaining Configurations and Firmware”](#), provides information about uploading and downloading configuration files and downloading firmware.
- [Chapter 5, “Managing Your Ports”](#), provides information about managing FC and GbE ports.
- [Chapter 6, “Administering ISL Trunking”](#), provides information on managing the optionally licensed ISL Trunking feature.
- [Chapter 7, “Managing Administrative Domains”](#), provides information on managing Admin Domains.
- [Chapter 8, “Administering Zoning”](#), provides information on how to use the Brocade Advanced Zoning feature to partition your storage area network (SAN) into logical groups of devices that can access each other.
- [Chapter 9, “Monitoring Performance”](#), provides information on how to use the Brocade Advanced Performance Monitoring feature to monitor your fabric performance.

- [Chapter 10, “Using the FC-FC Routing Service,”](#) provides information on using the FC-FC Routing Service to share devices between fabrics without merging those fabrics.
- [Chapter 11, “Working With Diagnostic Features,”](#) provides information about trace dumps, viewing switch health, and interpreting the LEDs.
- [Chapter 12, “Administering Fabric Watch,”](#) provides information on how to use the Fabric Watch feature to monitor the performance and status of switches and alert you when problems arise.
- [Chapter 13, “Administering Extended Fabrics,”](#) provides information on how to configure a port for long distance.
- [Chapter 14, “Administering the iSCSI Target Gateway,”](#) provides information on how to configure and manage the iSCSI Target Gateway.
- [Chapter 15, “Using the Access Gateway,”](#) provides information on how to configure and manage the Brocade Access Gateway.
- [Chapter 16, “Routing Traffic,”](#) provides information on how to configure routes.
- [Chapter 17, “Configuring Standard Security Features,”](#) provides information on managing user accounts, SNMP, and RADIUS server.
- [Chapter 18, “Administering FICON CUP Fabrics,”](#) provides information on how to administer and manage FICON CUP fabrics. You can enable FMS mode, edit and create configurations, and edit FMS parameters.
- [Chapter 19, “Limitations,”](#) discusses limitations of and provides workarounds for using Web Tools.

Supported hardware and software

This document supports the following platforms:

- Brocade 200E switch
- Brocade 3250 switch
- Brocade 3850 switch
- Brocade 3900 switch
- Brocade 4012
- Brocade 4016
- Brocade 4018
- Brocade 4020
- Brocade 4024
- Brocade 4100 switch
- Brocade 5000 switch
- Brocade 4900 switch
- Brocade 7500 switch
- Brocade 7600 switch
- Brocade 24000 director
- Brocade 48000 director

In those instances in which procedures or parts of procedures documented here apply to some switches but not to others, this guide identifies exactly which switches are supported and which are not.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for 5.3.0, documenting all possible configurations and scenarios is beyond the scope of this document.

This document does not support all Fabric OS versions. This document is specific to Fabric OS 5.3.0. To obtain information about an OS version other than 5.3.0, refer to the documentation specific to that OS version.

What's new in this document

The following changes have been made since this document was last released:

- Information that was added:
 - New chapter, "Using the Access Gateway," was added to described enhanced Access Gateway support
 - Text describing managing blades
 - Support for Brocade 5000, 4024, 4020, 4018, 4016, and 4012
 - Support for IPv6
 - Support to download firmware to an AP blade
 - New IP Filter support
 - New iSCSI wizard for setup
 - Port Administration now supports FC Fastwrite
- Information that was changed:
 - All screens showing the software have been updated to reflect the new interface
 - All procedures describing the interface have been updated
 - Reboot/Fastboot functionality has been moved from the SA firmware download panel to the SA Switch panel.
 - Zone views are streamlined from four to two views.
- Information that was removed:
 - A chapter titled "Using the FCIP Tunneling Service" was removed because this feature was removed from Web Tools.
 - Information about Quickloops and Fabric Assist zoning

For further information, refer to the release notes.

Document conventions

This section describes text formatting conventions and important notices formats.

TEXT FORMATTING

The narrative-text formatting conventions that are used in this document are as follows:

bold text	Identifies command names Identifies the names of user-manipulated GUI elements Identifies keywords and operands Identifies text to enter at the GUI or CLI
<i>italic text</i>	Provides emphasis Identifies variables Identifies paths and Internet addresses Identifies document titles
code text	Identifies CLI output Identifies syntax examples

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, **switchShow**. In actual examples, command lettercase is often all lowercase. Otherwise, this manual specifically notes those cases in which a command is case sensitive.

NOTES, CAUTIONS, AND WARNINGS

The following notices appear in this document.

NOTE

A note provides a tip, emphasizes important information, or provides a reference to related information.

CAUTION

A caution alerts you to potential damage to hardware, firmware, software, or data.

WARNING

A warning alerts you to potential danger to personnel.

KEY TERMS

For definitions specific to Brocade and Fibre Channel, see the *Brocade Glossary*.

For definitions of SAN-specific terms, visit the Storage Networking Industry Association online dictionary at:

<http://www.snia.org/education/dictionary>

Additional information

This section lists additional Brocade and industry-specific documentation that you might find helpful.

BROCADE RESOURCES

The following related documentation is provided on the Brocade Documentation CD-ROM and on the Brocade Web site, through Brocade Connect.

NOTE

Go to <http://www.brocade.com> and click **Brocade Connect** to register at no cost for a user ID and password.

Fabric OS

- *Fabric OS Administrator's Guide*
- *Fabric OS Command Reference*
- *Fabric OS MIB Reference*
- *Fabric OS Message Reference*
- *Brocade Glossary*

XPath OS

- *XPath OS Administrator's Guide*
- *XPath OS Command Reference*
- *XPath OS MIB Reference*
- *XPath OS System Error Message Reference*
- *Web Tools—AP Edition Administrator's Guide*

Fabric OS Optional Features

- *EZSwitchSetup Administrator's Guide*
- *Fabric Watch Administrator's Guide*
- *Fabric Manager Administrator's Guide*
- *Secure Fabric OS Administrator's Guide*

Brocade 48000

- *Brocade 48000 Hardware Reference Manual*
- *Brocade 48000 QuickStart Guide*
- *FR4-18i Hardware Reference Manual*
- *FC4-48 Hardware Reference Manual*

Brocade 24000

- *Brocade 24000 Hardware Reference Manual*
- *Brocade 24000 QuickStart Guide*

Brocade 24000/48000

- *Port Blade and Filler Panel Replacement Procedure*
- *Control Processor Blade Replacement Procedure*
- *Blower Assembly Replacement Procedure*
- *Cable Management Tray and Guide Replacement Procedure*
- *Chassis Door Replacement Procedure*
- *WWN Bezel and Card Replacement Procedure*
- *Power Supply and Filler Panel Replacement Procedure*
- *14U Rack Mount Kit Installation Procedure*
- *Mid-Mount Rack Kit Installation Procedure*

Brocade 7500

- *Brocade 7500 Hardware Reference Manual*
- *Brocade 7500 QuickStart Guide*
- *Brocade 7500 Fan Assembly Replacement Procedure*
- *Brocade Mid Sized Power Supply Replacement Procedure*

Brocade 5000

- *Brocade 5000 Hardware Reference Manual*
- *Fixed Rack Mount Kit Installation Procedure*
- *Brocade 5000 Mounting Ears Installation Procedure*
- *Brocade 5000 Power Supply and Fan Assembly Replacement Procedure*
- *Brocade 5000 QuickStart Guide*
- *Slide Rack Mount Kit Installation Procedure*

Brocade 4900

- *Brocade 4900 Hardware Reference Manual*
- *Brocade 4900 QuickStart Guide*
- *Brocade 4900 Fan Assembly Replacement Procedure*
- *Brocade Mid Sized Power Supply Replacement Procedure*

Brocade 4100

- *Brocade 4100 Hardware Reference Manual*
- *Brocade 4100 QuickStart Guide*

Brocade 4020

- *Brocade 4020 Hardware Reference Manual*
- *Brocade 4020 QuickStart Guide*

Brocade 4016

- *Brocade 4016 Hardware Reference Manual*
- *Brocade 4016 QuickStart Guide*

Brocade 3900

- *Brocade 3900 Hardware Reference Manual* (for v4.x software)
- *Brocade 3900 QuickStart Guide* (for v4.x software)
- *Brocade 3900 Fan Assembly Replacement Procedure*
- *Brocade 3900 Motherboard Assembly Replacement Procedure*
- *Brocade 3900 Power Supply Replacement Procedure*

Brocade 3250/3850

- *Brocade 3250/3850 Hardware Reference Manual* (for v4.x software)
- *Brocade 3250/3850 QuickStart Guide* (for v4.x software)

Brocade 200E

- *Brocade 200E Hardware Reference Manual* (for v5.x software)

Brocade Multiprotocol Router Model AP7420

- *Brocade Multiprotocol Router Model AP7420 Hardware Reference Manual*
- *Brocade Multiprotocol Router Model AP7420 QuickStart Guide*
- *Brocade Multiprotocol Router Model AP7420 Power Supply Replacement Procedure*
- *Brocade Multiprotocol Router Model AP7420 Fan Assembly Replacement Procedure*

For practical discussions about SAN design, implementation, and maintenance, you can obtain *Building SANs with Brocade Fabric Switches* through:

<http://www.amazon.com>

For additional Brocade documentation, visit the Brocade SAN Info Center and click the Resource Library location:

<http://www.brocade.com>

Release notes are available on the Brocade Connect Web site and are also bundled with the Fabric OS firmware.

OPTIONAL BROCADE FEATURES

Optional Brocade features include:

Advanced Performance Monitoring

Enables more effective end-to-end SAN performance analysis to enhance performance tuning, increase productivity, optimize resource utilization, and reduce costs.

Extended Fabrics

Supports the reliable, high-speed connectivity of Brocade switches over dark fiber or Dense Wave Division Multiplexing (DWDM) equipment at distances up to 500 kilometers to enhance business continuance operations.

Fabric Watch

Continuously monitors SAN fabrics for potential faults based on thresholds set for a variety of SAN fabric elements and events—automatically alerting administrators to potential problems before they become costly failures.

ISL Trunking	Optimizes the performance and availability of SAN fabrics while simplifying ISL management. Two 4 Gbit/sec Brocade switches can automatically group up to eight ISLs into a single logical trunk with a total throughput of up to 32 Gbit/sec.
Advanced Zoning	Automatically groups SAN fabric-connected devices into logical zones that restrict access to member devices in the zone. Advanced Zoning uses hardware enforcement at both the port and WWN level to provide more robust data protection.
Secure Fabric OS	Provides a comprehensive security solution to help protect mission-critical data. Key features include centralized policy-based security management, management data encryption, and authentication to create a fabric-wide trusted environment with control over all levels of fabric access and communication.
FICON® CUP	Enables IBM host-based management programs to manage FICON fabric switches in-band by sending commands to the Fabric OS emulated control device.

OTHER INDUSTRY RESOURCES

For additional resource information, visit the Technical Committee T11 Web site. This Web site provides interface standards for high-performance and mass storage applications for Fibre Channel, storage management, and other applications:

<http://www.t11.org>

For information about the Fibre Channel industry, visit the Fibre Channel Industry Association Web site:

<http://www.fibrechannel.org>

Getting technical help

Contact your switch support supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information available:

1. General Information

- Technical Support contract number, if applicable
- Switch model
- Switch operating system version
- Error numbers and messages received
- **supportSave** command output
- Detailed description of the problem and specific questions
- Description of any troubleshooting steps already performed and results
- Serial console and telnet session logs
- syslog message logs

2. Switch Serial Number

The switch serial number and corresponding bar code are provided on the serial number label, as shown here:



The serial number label is located as follows:

- *Brocade 200E, 3200, 3250, 3850, 4012, 4016, 4018, 4020, and 4024*—On the bottom of the chassis
- *Brocade 3800 and 3900*— Nonport side of the chassis
- *Brocade 4100, 4900, 5000, 7500, and 7600*—On the switch ID pull-out tab located inside the chassis on the port side on the left
- *Brocade 12000, 24000, and 48000*—Inside the chassis next to the power supply bays
- *Brocade Multiprotocol Router Model AP7420*—On the bottom of the chassis and on the back of the chassis.

3. World Wide Name (WWN)

- *Brocade 200E, 3250, 3800, 3850, 3900, 4012, 4016, 4018, 4020, 4024, 4100, 4900, 5000, 7500, 7600 switches and Brocade 24000, and 48000 directors*: Provide the license ID. Use the **licenseIdShow** command to display the license ID.
- *Brocade Multiprotocol Router Model AP7420*: Provide the switch WWN. Use the **switchShow** command to display the switch WWN.
- *All other Brocade switches*: Provide the switch WWN. Use the **wwn** command to display the switch WWN.

Document feedback

Because quality is our first concern at Brocade, we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. Forward your feedback to:

documentation@brocade.com

Provide the title and version number and as much detail as possible about your comment, including the topic heading and page number and your suggestions for improvement.

Introducing Web Tools

Brocade Web Tools is a graphical user interface (GUI) that enables administrators to monitor and manage single or small fabrics, switches, and ports from a standard workstation. It is an optionally licensed product that runs on Brocade Fabric OS.

Web Tools provides the administrative control point for Brocade Advanced Fabric Services, including Advanced Zoning, ISL Trunking, Advanced Performance Monitoring, and Fabric Watch. Web Tools also provides an interface to telnet commands to perform special switch functions and diagnostics that are available only through the telnet interface.

For some switch models, Web Tools provides a simplified interface, EZSwitchSetup, that allows less-experienced users to perform basic management tasks. See the *EZSwitchSetup Administrator's Guide* for information about the EZSwitchSetup interface.

In this chapter

This chapter contains the following sections:

- [Requirements, installation, and support](#) 1
- [Launching Web Tools](#) 8
- [Administrative domains](#) 9
- [Role-Based access control](#) 11
- [Session management](#) 12

Requirements, installation, and support

Before you install Web Tools on your workstation, verify that your switches and workstation meet the Web Tools requirements listed in this chapter.

This section contains the following subsections:

- [“Requirements,”](#) next
- [“Installing a Web Tools license”](#) on page 6
- [“Value line licenses”](#) on page 8

REQUIREMENTS

Web Tools requires any browser that conforms to HTML version 4.0, JavaScript version 1.0, and Java Plug-in 1.4.2_08 or higher.

Brocade has certified and tested Web Tools on the platforms shown in [Table 1](#).

TABLE 1 Certified and tested platforms

Operating System	Browser	Java Plug-In ¹
Solaris 10	Firefox 2.0	1.5.0_06
Linux Red Hat AS4	Firefox 2.0	1.5.0_06
Windows 2003 Server, SP1	Internet Explorer 7.0	1.5.0_06
Windows XP, SP2	Internet Explorer 7.0	1.5.0_06

1. Java Plug-in 1.4.2_08 is also supported, although Java Plug-in 1.5.0_06 is the only version that has been certified and fully tested.

TABLE 2 Supported platforms

Operating System	Browser	Java Plug-In
RH Enterprise Linux AS3	Firefox 2.0	1.5.0_06
Windows 2000, SP4	Firefox 2.0, Internet Explorer 6.0	1.5.0_06
Windows 2003 Server, SP1	Firefox 2.0, Internet Explorer 6.0	1.5.0_06
Windows XP, SP2	Firefox 2.0, Internet Explorer 6.0	1.5.0_06

NOTE

Some browsers must be configured to work with Web Tools. For information about how to do this, see [“Configuring Internet Explorer,”](#) next.

Adequate RAM is required on Windows systems:

- 256 MB or more RAM for fabrics comprising 15 switches or less
- 512 MB or more RAM for fabrics comprising more than 15 switches

A minimum of 8 MB of video RAM is also recommended.

Configuring Internet Explorer

Correct operation of Web Tools with Internet Explorer requires specifying the appropriate settings for browser refresh frequency and process model. Browser pages should be refreshed frequently to ensure the correct operation of Web Tools.

To set the refresh frequency

1. Click **Tools > Internet Options** in the browser.
2. Click the **General** tab and click **Settings** under “Temporary Internet Files.”
3. Click **Every visit to the page** under “Check for newer versions of stored pages,” as shown in [Figure 1](#) on page 3.

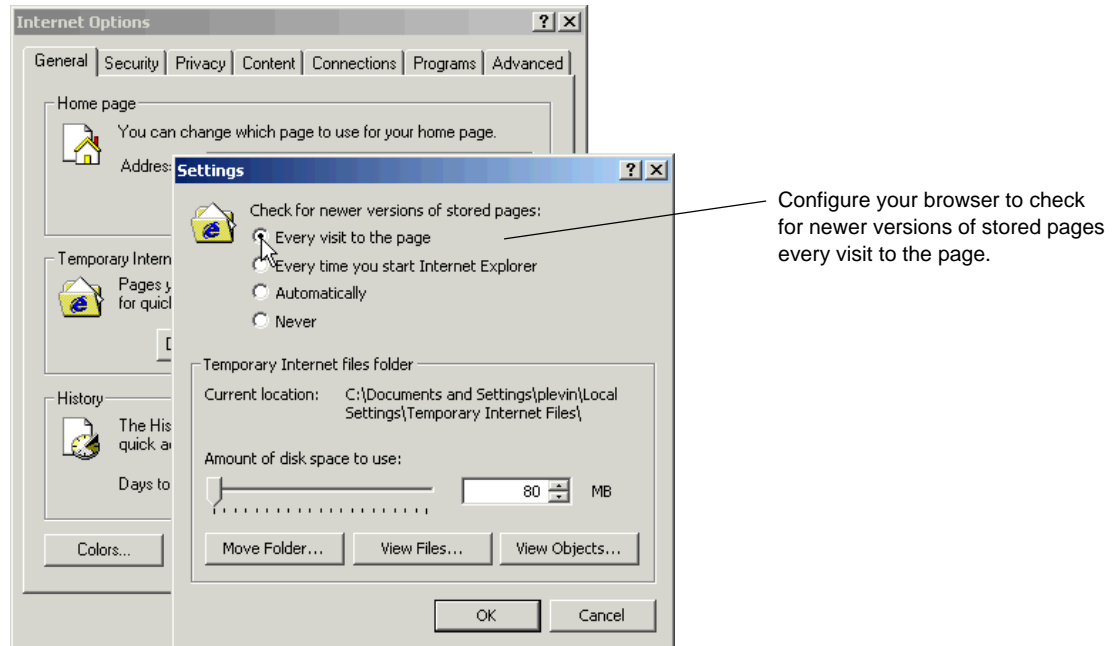


FIGURE 1 Configuring Internet Explorer

Installing Java on the workstation

Java Plug-in version 1.5.0_06 must be installed on the workstation for the correct operation of Web Tools. Java Plug-in version 1.4.2_08 is also supported.

If you try to launch Web Tools without any Java Plug-in installed,

- Internet Explorer automatically prompts and downloads the proper Java Plug-in.
- Firefox downloads the most recently released Java Plug-in.

If you try to launch Web Tools with an earlier version Java Plug-in installed,

- Internet Explorer might prompt for an upgrade, depending on the existing Java Plug-in version.
- Firefox uses the existing Java Plug-in.

To install the JRE on your Solaris or Linux client workstation

1. Locate the JRE on the Internet, at the following URL:

http://java.sun.com/products/archive/j2se/5.0_06/index.html

NOTE

This URL points to a non-Brocade Web site and is subject to change without notice.

2. Select **JRE 5.0 Update 6**.

1 Requirements, installation, and support

3. Follow the instructions to install the JRE.
4. Create a symbolic link from this location...

`$FIREFOX/plugins/libjavaplugin_oji.so`

...to this location:

`$JRE/plugin/$ARCH/ns600/libjavaplugin_oji.so`

To install patches on Solaris

1. Search for any required patches for your current version of the JRE at the following Web site:

<http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage>

NOTE

This URL points to a non-Brocade Web site and is subject to change without notice.

2. Follow the link to download the patch, and exit the browser when done.
3. Install the patch and reboot the system.

To install the Java plug-in on Windows

1. Click **Start Menu > Settings > Control Panel** and select the Java Plug-in Control Panel.
2. Click the **About** tab.
3. Determine whether the correct Java Plug-in version is installed:
 - If the correct version is installed, Web Tools is ready to use.
 - If no Java Plug-in is installed, point the browser to a switch running Fabric OS 5.2.0 or later to install JRE 1.5.0_06. Web Tools will guide you through the steps to download the proper Java Plug-in.
 - If an outdated version is currently installed, uninstall it, reboot your personal computer, relaunch the browser, and enter the address of a switch running Fabric OS 5.2.0 or later to install JRE 1.5.0_06. Web Tools will guide you through the steps to download the proper Java Plug-in.

Configuring the Java plug-in

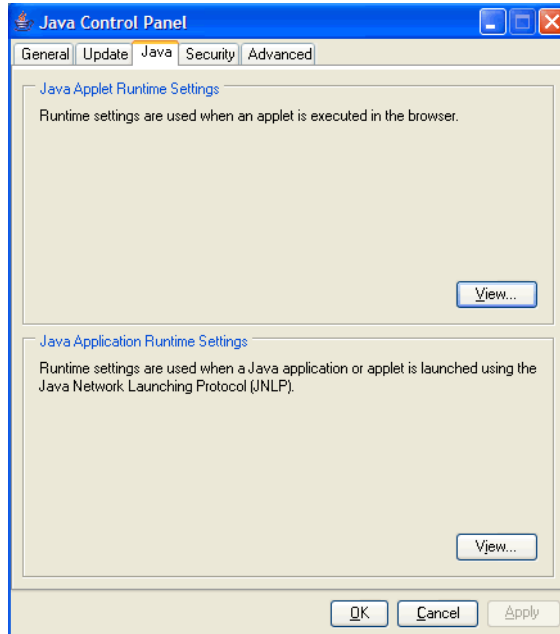
If you are managing fabrics with more than 10 switches or 1000 ports, or if you are using the iSCSI Gateway module extensively, you should increase the default heap size to 256 MB to avoid out-of-memory errors.

If you are using a Mozilla family browser (Firefox, Netscape), you should set the default browser in the Java control panel.

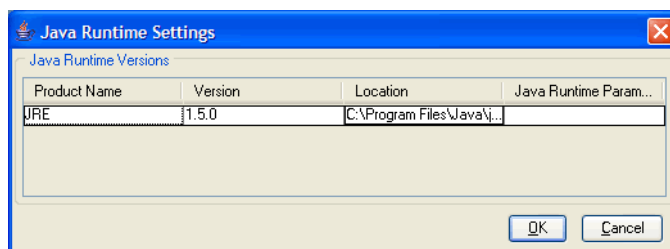
The following procedures instruct you in increasing the default heap size in the Java Control Panel and in setting the default browser.

To configure the Java plug-in on Windows

1. From the **Start** menu button, select **Settings > Control Panel > Java**.
2. Click the **Java** tab.

**FIGURE 2** Java Control Panel

3. In the section **Java Applet Runtime Settings**, click **View**
The Java Runtime Settings dialog box displays.

**FIGURE 3** Java Runtime Settings

4. Double-click in the Java Runtime Parameters field and type the following information to set the minimum and maximum heap size:

-Xms256m -Xmx256m

In this example, the minimum and maximum sizes are both 256 MB.
5. Click **Apply** to apply your settings and close the Java Control Panel.

1 Requirements, installation, and support

To configure the Java plug-in for Mozilla family browsers

1. From the **Start** menu button, select **Settings > Control Panel**
2. Click the **Advanced** tab and expand the **Default Java for browsers** option.

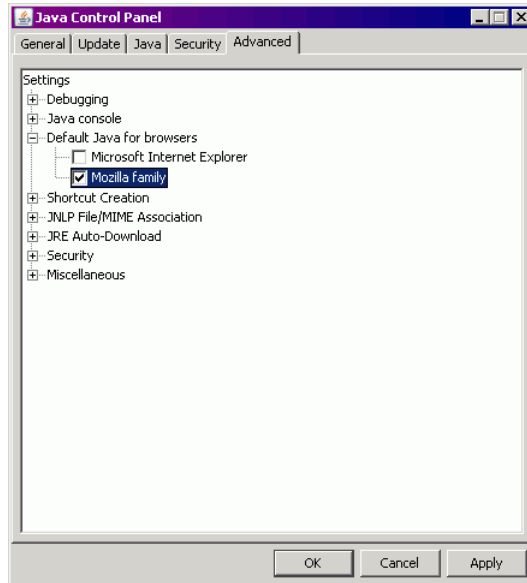


FIGURE 4 Default Java for browsers option

3. Select Mozilla family and click **OK**.
4. Click **Apply** to apply your settings and close the Java Control Panel.

INSTALLING A WEB TOOLS LICENSE

You can install a Web Tools license either through telnet or over the Web. License keys are provided on a per-chassis basis, so for products that support multiple logical switches (domains), a license key applies to all domains within the chassis.

To determine whether a license is already installed on a switch, follow the instructions provided under [“Installing a Web Tools license through telnet,”](#) next. If a license is not installed, contact your switch supplier to obtain a license key.

Installing a Web Tools license through telnet

Use the following procedure to determine whether a Web Tools license is installed on your switch and, if not, install it.

To install a Web Tools license through telnet

1. Log in to the switch via telnet (see the *Fabric OS Administrator's Guide* for more information), using an account that has administrative privileges.
2. To determine whether a Web Tools license is already installed on the switch, type **licenseShow** on the telnet command line.

A list displays, showing all the licenses currently installed on the switch:

```
switch:admin> licenseshow
1A1AaAaaaaAAA1a: ]—This is the license key (excluding the colon). The installed feature is listed below.
    Zoning license
1A2AaAbbbbBBB1a:
    SES license
1A3AaAbcbBBCC1d:
    QuickLoop license
```

If the Web Tools license is not included in the list or is incorrect, continue with step 3.

3. On the command line, type...:

```
licenseadd key
```

...where *key* is the license key. The license key value is case-sensitive and must be entered exactly as given.

4. Verify that the license was added by typing the following command:

```
licenseshow
```

If the Web Tools license is listed, the feature is available. If the license is not listed, repeat [step 3](#).

Installing a Web Tools license through the Web

If you launch Web Tools from any nonlicensed switch, the software automatically displays the license dialog box. If the fabric already contains at least one licensed switch, you can use Web Tools to view and license other switches from the licensed switch.

If you do not have a switch that has a Web Tools license installed on it, Web Tools is active for only 30 days from the date that the switch is activated. After the 30 day period, the Web Tools functionality is disabled and error messages will appear in the logs, and on the console, to inform you that need a Web Tools license to access the feature.

To install the first license through the Web

1. Launch the Web browser and type the IP address of the switch in the **Location/Address** field:

```
http://10.77.77.77
```

2. Press **Enter**.

If a Web Tools license is already installed on the switch, Web Tools launches. If no license is installed, a license dialog box displays.

3. If the license dialog box displays, follow the instructions provided.

To install other licenses through the Web

1. Launch the Web browser and type the IP address of the licensed switch in the **Location/Address** field:

```
http://10.77.77.77
```

2. Press **Enter**.
3. On Web Tools Switch Explorer, click the switch to which you want to add a license.
4. On the licensing window, follow the instructions that are provided.

VALUE LINE LICENSES

If your fabric includes a switch with a limited switch license and you are launching Web Tools using that switch, if the fabric exceeds the switch limit indicated in the license, Web Tools allows a 30-day “grace period” in which you can still monitor the switch through Web Tools. However, Web Tools will display warning messages periodically.

These messages warn you that your fabric size exceeds the supported switch configuration limit and tells you how long you have before Web Tools will be disabled. After the 30-day grace period, you will no longer be able to launch Web Tools from the switch with the limited switch license if that switch is still exceeding the switch limit.

Value line fabric licensing is applicable only to Brocade 3250 and 3850 switches. These licenses are indicated by “2 Domain Fabric” and “4 Domain Fabric” in the **License** tab of the Switch Administration window. See [“Managing licensed features”](#) on page 43 for more information.

Web Tools is part of the Fabric OS of a switch. When you launch Web Tools on a switch, you can manage other switches in the fabric that have lower or higher firmware versions. It is important to note that when accessing these switches you are opening the remote switch’s version of Web Tools, and the functionality available for those switches might vary.

Launching Web Tools

You can launch Web Tools on any workstation with a compatible Web browser installed. For a list of Web browsers compatible with Fabric OS 5.3.0, see [Table 1](#). Web Tools also supports HTTPS protocol, if that protocol is enabled for the switch. For more information on enabling the HTTPS protocol on your switch, see the *Fabric OS Administrator’s Guide*.

To launch Web Tools

1. Launch the Web browser and type the IP address of the licensed switch in the **Address** field:

`http://10.77.77.77`

or

`https://10.77.77.77`

2. Press **Enter**.

A browser window opens to launch Web Tools. A Login dialog box opens. See [“Logging In”](#) on page 12 for more information. The browser window is left open. You can close it anytime after the Login dialog box appears.

What happens next depends on the switch type:

- **For the Brocade 200E, 3250, 4012, 4016, 4018, 4020, 4024, 4100, 4900, and 5000 switches**, one of the following launches, depending on the switch configuration:

- EZSwitchSetup Switch Manager

This interface launches if the switch has already been set up and is configured with EZSwitchSetup. See the *EZSwitchSetup Administrator’s Guide* for information about the EZSwitchSetup interface.

If you want to use Web Tools instead of EZSwitchSetup, click **Advanced Management** in the lower-left corner of this window to launch the Web Tools interface.

- Web Tools (see [Figure 5](#) on page 9)

This interface opens if the switch is configured with the command line interface (CLI) or Web Tools.

- **For the Brocade AP7420**, the Web Tools—AP Edition interface launches. See the *Web Tools—AP Edition Administrator's Guide* for information on using the Web Tools—AP Edition interface for the Brocade AP7420.
- **For all other switches**, the Web Tools interface opens.

This book describes only the Web Tools interface.

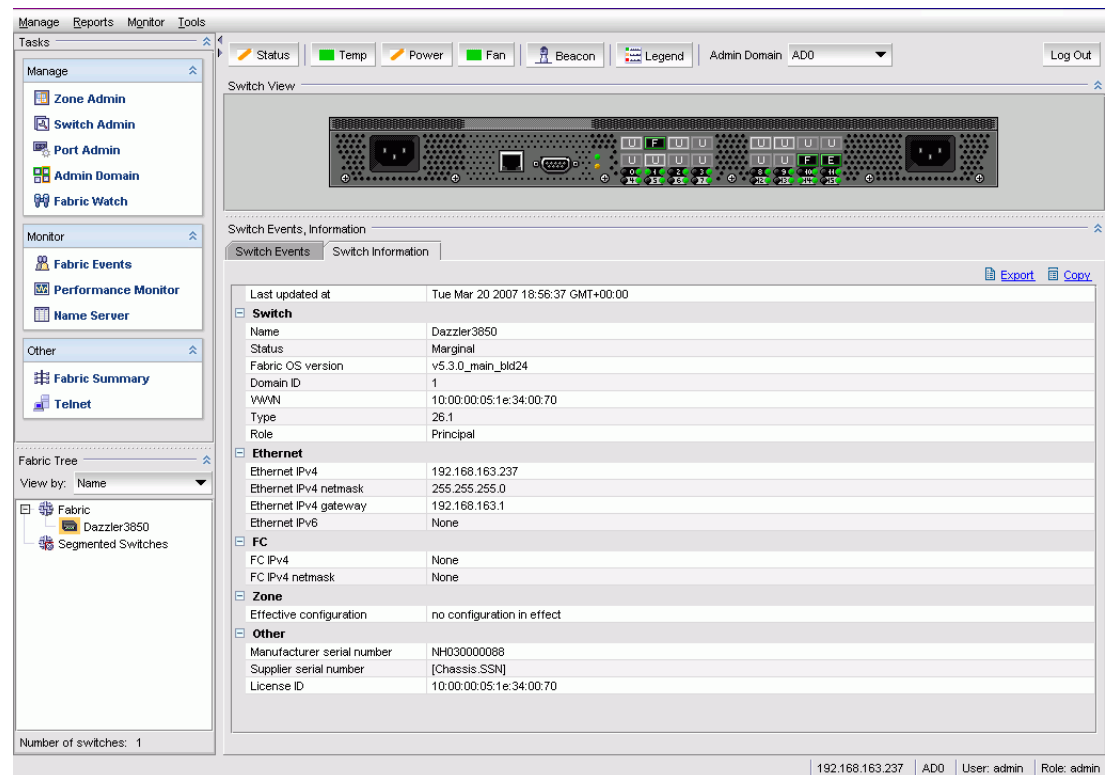


FIGURE 5 Web Tools interface

Administrative domains

An “administrative domain” (Admin Domain or AD) is a logical grouping of fabric elements that defines what switches, ports, and devices you can view and modify. An Admin Domain is a filtered administrative view of the fabric. The logical view presented within an Admin Domain does not hide fabrics, chassis, switches, and slots; however, the attributes of switch ports and end devices are filtered based on Admin Domain membership.

1 Administrative domains

Admin Domains permit access to a configured set of users. If a switch is part of an Admin Domain, then when you log in with an account that has an administrator role, you can perform switch enable and disable functions and all switch port-level functions such as port enable and port disable. You cannot perform fabric-wide management, as switch membership within a zone does not provide zoning rights on the switch ports.

NOTE

Do not confuse an Admin Domain with the domain ID of a switch. They are two different identifiers.

Admin Domains are identified by a numeric ID (0–255) and also by name. This name can be autogenerated based on the ID (for example AD1 or AD5) or you can specify a more informative name such as Accounting or Engineering.

AD0 is a special Admin Domain that contains all switches, ports, and devices that have not been put into other Admin Domains. AD255, another special domain, is an unfiltered view of the entire physical fabric.

NOTE

Some features work only in AD255 when user-defined domains are present, such as ACL management.

By default, all fabric elements belong to AD0. In Fabric OS v5.2.0 and higher, a physical fabric administrator with appropriate permissions can create up to 254 additional Admin Domains and assign fabric resources to them (see [Chapter 7, “Managing Administrative Domains”](#)). Only users who have been specifically assigned to those domains can view and modify the resources they contain.

ADMIN DOMAINS AND LOGIN

You are always logged in to an Admin Domain, and you can view and modify only the devices in that Admin Domain.

You can log in to only one Admin Domain at a time. When you log in, you select the Admin Domain that you want to manage. You can later change the Admin Domain to which you are logged in.

If you have more than one Admin Domain, one of them will have been specified as your “home Admin Domain.” Your home Admin Domain is the one you are automatically logged in to unless you explicitly select a different one. If a home Admin Domain is deleted or deactivated, then by default you will be logged in to the lowest numbered Admin Domain in your Admin Domain list. A home Admin Domain, like the Admin Domain list, is a configurable property of a non-default user account.

For default accounts such as admin and user, the home Admin Domain defaults to AD0 and cannot be changed. For user-defined accounts, the home Admin Domain also defaults to 0 but an administrator can set the home Admin Domain to any Admin Domain to which the account has been given access. The Admin Domain List for default admin accounts is 0–255, which gives automatic access to any Admin Domain as soon as it is created, and makes them physical fabric administrators. The Admin Domain list for the default user account is AD0 only. The Admin Domain list property for default accounts also cannot be changed.

A “physical fabric administrator” is an admin role user whose account has access to all Admin Domains (AD0-255) as soon as they are created. Only physical fabric administrators can create, modify, delete, and activate or deactivate Admin Domains.

ADMIN DOMAINS AND SWITCH WWN

Admin Domains are treated as fabrics. Because switches cannot belong to more than one fabric, switch WWNs (world-wide names) are converted so that they appear as unique entities in different Admin Domains (fabrics).

The switch WWN is in the following format:

`10:00:nn:nn:nn:nn:nn:nn`

In an Admin Domain context, the switch WWN is converted from NAA=1 to NAA=5 format, with the Admin Domain number added, using the following syntax:

`5n:nn:nn:nn:nn:nn:nn:n9:xx`

where `xx` is the AdminDomain_number.

For example, if the switch WWN is:

`10:00:00:60:69:e4:24:e0`

then the converted WWN for that switch in AD1 is:

`50:06:06:9e:42:4e:09:01`

ADMIN DOMAINS AND ZONING

Each Admin Domain has its own zone database, with both defined and effective zone configurations and all related zone objects (zones, zone aliases, and zone members). Within an Admin Domain, you can configure zoning only with the devices that are present in that Admin Domain.

Before you implement Admin Domains, you must set the default zoning mode. See [“Implementing administrative domains”](#) on page 83 for additional information.

You cannot perform any zoning operations from AD255.

Role-Based access control

Role-Based Access Control (RBAC) defines the capabilities that a user account has based on the role the account has been assigned. For each role, there is a set of pre-defined permissions on the jobs and tasks that can be performed on a fabric and its associated fabric elements.

When you log in to a switch, your user account is associated with a pre-defined role. The role that your account is associated with determines the level of access you have on that switch and in the fabric. Following is a description of each of the roles:

admin	You have full access to all of the Web Tools features.
operator	You can perform any actions on the switch that do not affect the stored configuration.
securityadmin	You can perform actions that do not affect the stored configuration.

1 Session management

switchadmin	You can perform all actions on the switch, except the following: <ul style="list-style-type: none">• You cannot modify zoning configurations.• You cannot create new accounts.• You cannot view or change account information for any accounts. You can only view your own account and change your account password.
zoneadmin	You can only create and modify zones.
fabricadmin	You can do everything the Admin role can do except create new users.
basicswitchadmin	You have a subset of Admin level access.
user	You have nonadministrative access and can perform tasks such as monitoring system activity.

For information about changing user account roles, see [“Creating and maintaining user-defined accounts”](#) on page 201.

Session management

A Web Tools session is the connection between the Web Tools client and its managed switch. A session is established when you log in to a switch through Web Tools. When you close Switch Explorer, Web Tools ends the session.

A session remains in effect until one of the following happens:

- You log out
- You close the Switch Explorer window
- The session ends due to inactivity (time out)

A session automatically ends if there has been no information sent to the switch for more than two hours. Because user key strokes are not sent to the switch until you apply or save the information, it is possible for your session to end while you are entering information in the interface. For example, entering a zoning scheme in the Zoning module does not require you to send information to the switch until you save the scheme.

Web Tools does not display a warning when the session is about to time out. If your session ends due to inactivity, must restart Web Tools and log in again.

Web Tools enables sessions to both secure and nonsecure switches.

Access rights for your session are determined by your role-based access rights and by the contents of your selected Admin Domain. After you log in, you can change to a different Admin Domain at any time; however, you cannot change your role-based permissions.

LOGGING IN

When you use Web Tools, you must log in before you can view or modify any switch information. This section describes the login process.

Prior to displaying the login window, Web Tools displays a security banner (if one is configured for your switch), which you must accept before logging in. The security banner displays every time you access the switch.

When you are presented with the login screen you must provide a user name and a password. Your home Admin Domain is automatically selected. You can optionally specify an Admin Domain other than your home domain.

Upon successful login, you are logged in to the specified Admin Domain.

NOTE

You must log in before you can view Switch Explorer (shown in [Figure 5](#) on page 9).

To log in

1. Click **Run** on the signed certificate applet

If you select the check box **Always trust content from this publisher**, the dialog box will not be displayed when you launch Web Tools again.

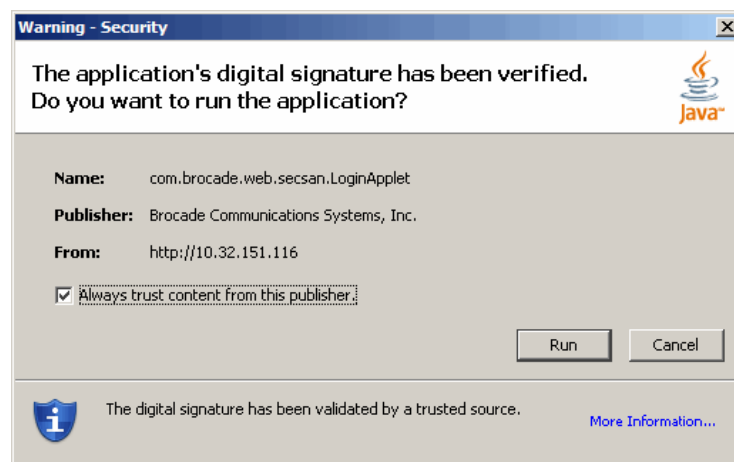


FIGURE 6 Signed applet certificate

2. Click **OK** in the security banner window, if one appears.

The login dialog box displays.

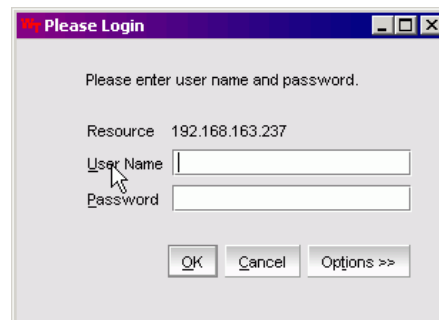


FIGURE 7 Login dialog box

3. Type your user name.
4. Type the password.

If your current password has expired, you must also provide a new password and confirm the new password.

1 Session management

Optional: Click **Options** to select an Admin Domain other than your default home domain.

The Login dialog box displays the Admin Domain options.

- Click the **Home Domain** radio button to log in to your default Admin Domain.
- Click the **User Specified Domain** radio button to log in to another Admin Domain instead of your home domain. Type the Admin Domain name or number.

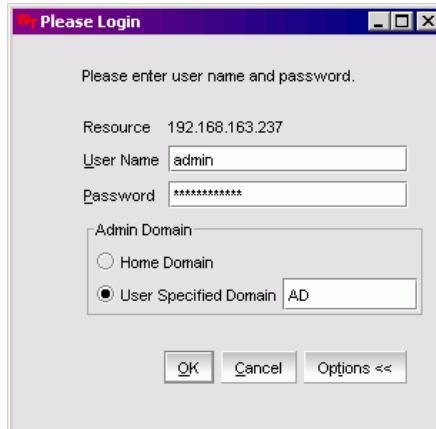


FIGURE 8 Login dialog box with Admin Domain options

5. Click **OK** (or click **Change Password and Login** if you have changed your password).

If the user name or password is incorrect, a dialog box displays indicating an authentication failure.

If you entered valid credentials, but specified an invalid Admin Domain, a dialog box displays from which you can choose a valid Admin Domain or click **Cancel** to log in to your home domain.

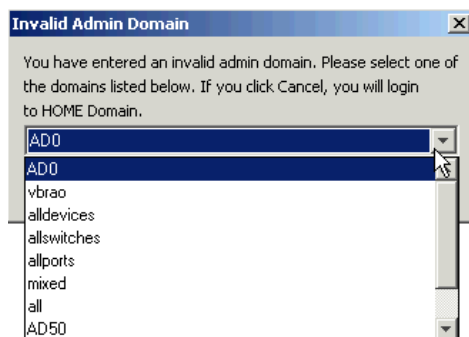


FIGURE 9 Invalid Admin Domain dialog box

LOGGING OUT

You can end a Web Tools session either by logging out or by closing Switch Explorer browser window.

Sometimes you might be logged out of a session involuntarily, without explicitly clicking the **Logout** button. You are automatically logged out when:

- A physical fabric administrator changes the contents of your currently selected Admin Domain.
- Your currently selected Admin Domain is removed or invalidated.
- Your currently selected Admin Domain is removed from your Admin Domain list.
- You initiate a firmware download from the Web Tools Switch Administration window. In this case, you are logged out a few minutes later when the switch reboots.
- Your session times out.

To end the Web Tools session

Perform one of the following:

- Click **Logout** in Switch Explorer.
- Click the X in the upper-right corner of Switch Explorer window to close it.
- Click **Cancel** on the log in the dialog box.
- Close *all* open Web Tools windows.

NOTE

When you click the Logout button in Switch Explorer, Web Tools might leave the Temperature, Fan, Power, or Fabric Event windows open. You must manually close these windows.

REQUIREMENTS FOR IPV6 SUPPORT

The following lists requirements for Web Tools IPv6 support:

- In pure IPv6 environment, you must configure DNS maps to IPv6 address of the switch.
- The switch name is required to match DNS name that is mapped to IPv6 address.
- If both IPv4 and IPv6 addresses have been configured, Web Tools uses the IPv4 address to launch switch.
- Use a switch that has v5.3.0 or later release firmware to manage a mixed fabric of IPv4 and IPv6 switches.
- Switches running on version 5.2.0 do not discover IPv6 address-only switches in the same fabric, until the IPv4 address has been configured.
- IPv6 address cannot be used to directly launch switch from Windows environment; it can be used in Unix and Linux environment.

1 Session management

Using the Web Tools Interface

In this chapter

This chapter contains the following sections:

- [Viewing Switch Explorer](#) 17
- [Displaying tool tips](#) 22
- [Refresh rates](#) 24
- [Displaying switches in the fabric](#) 24
- [Using Web Tools and secure mode](#) 25
- [Working with Web Tools: recommendations](#) 26

Viewing Switch Explorer

The first thing you see when you log in to a switch with Web Tools is Switch Explorer, shown in [Figure 10](#) on page 18. Switch Explorer is divided into areas that provide access to, and information about, the switch and fabric:

- Left Pane provides Tasks and Fabric Tree areas.
The Tasks area let you perform management, monitoring, and other tasks. The [Fabric Tree](#) displays a list of all the switches in the fabric.
- A menu bar, at the top of the window, provides access to commands and actions. The menu bar displays the same commands as the left pane of Switch Explorer. If you choose to collapse the left pane, you still have access to:
 - Management tasks, such as zone administration, switch administration, and port administration.
 - Reporting tasks, such as viewing a fabric summary or the status of a switch
 - Monitoring tasks, such as viewing fabric events, performance monitoring, and viewing the temperature or power status.
 - Tools tasks, such as opening the telnet window.
- [Switch View buttons](#) above Switch View provides access to switch information: status, temperature, power, and fan data, beaconing, and the legend for the Switch View.
Although clicking a button can open a separate dialog or window which you can perform management tasks, all access control is established when you first log in to the switch.
Buttons in Switch Explorer are unavailable for two reasons: your account does not have sufficient privileges to access this feature, or your currently selected Admin Domain does not meet some condition to access the feature.
- [Admin Domain Context](#) is a drop-down field which indicates the administrative domain you are viewing and allows you to change it.

2 Viewing Switch Explorer

- [Switch View](#) displays an interactive graphic of the switch.
- [Switch Events](#) and [Switch Information](#) are tabs that allow you to view event information and switch information, including connectivity, port, zone and other information.
- An indicator bar in the lower-right corner of every module window contains the Admin Domain you are currently in, the user name with which you logged in to the switch, and the role associated with your user account.

Use this table with [Figure 10](#) to identify the areas of Switch Explorer.

- 1 [Tasks](#) and [Fabric Tree](#)
- 2 [Menu bar](#)
- 3 [Switch View](#) buttons
- 4 [Admin Domain Context](#)
- 5 [Switch View](#)
- 6 [Switch Events and Switch Information](#)
- 7 [Indicator bar](#)

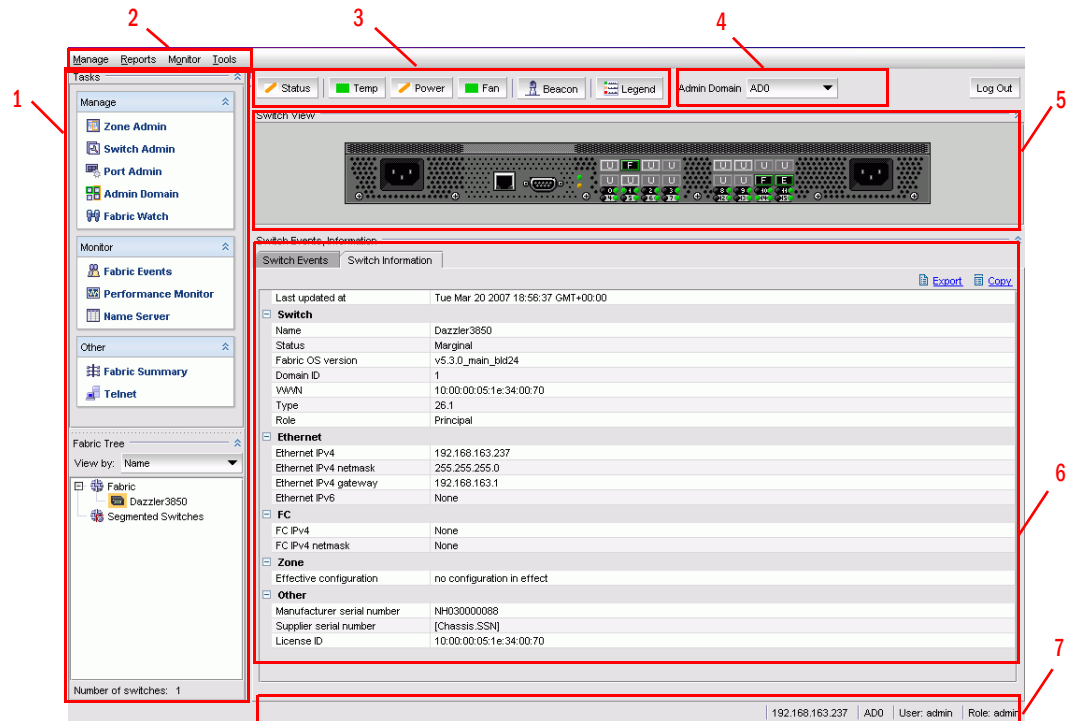


FIGURE 10 Switch Explorer

TASKS

The Tasks menu lets you manage, monitor, and perform other tasks.

Management section provides access to:

- Zone administration

This information is collected from the selected switch. This icon is displayed only if a Brocade Advanced Zoning license is installed on the switch. If secure mode (SFOS) is enabled, or if an ACL-based FCS policy is in effect, zoning can be administered only from the primary fabric configuration server (FCS) switch. If the selected switch has a zoning license installed but is not the primary switch, the Zone Admin icon is displayed but not activated. See [“Managing zoning with Web Tools”](#) on page 97 for more information

- Switch administration
- Port administration
- Admin Domain administration
- Fabric Watch

NOTE

Some of these functions require a license key to activate.

Monitor section provides access to

- Fabric events

This information is collected from the launch switch. See [“Monitoring events”](#) on page 48 for more information.

- Performance monitoring
- Name Server information

This information is collected from the selected switch. See [“Displaying the Name Server entries”](#) on page 53 for more information.

Other section provides access to:

- Fabric summary

This information is collected from the selected switch. See [“Displaying a fabric summary report”](#) on page 53 for more information.

- Telnet tools

NOTE

It is important to note that certain Fabric OS features are available only on particular switch types, and the system displays only the icons that are appropriate for the switch type.

FABRIC TREE

Fabric Tree displays all switches in the fabric, even those that do not have a Web Tools license and that are not owned by your selected Admin Domain. Switches that are not owned by the Admin Domain are shown in the Fabric Tree with switch status. Fabric Tree does not display switches segmented before Web Tools was launched.

Use the drop-down menu at the top of the Fabric Tree area to view switches in the Fabric Tree by switch name, IP address, or WWN. The background color of the switch icon indicates the current status of the switch. You can mouse over a switch to display the IP address and current status. To manually refresh the status of a switch within the fabric, right-click the switch in the Fabric Tree and choose **Refresh**.

Although Fabric Tree displays all the switches in the fabric, you can manage only the switches that have a Web Tools license installed. Other switches must be managed through the Fabric OS command line interface (CLI) or another management application. For information on adding a Web Tools license to a switch, see [“Installing a Web Tools license”](#) on page 6.

ADMIN DOMAIN CONTEXT

The Admin Domain field displays the currently selected Admin Domain and allows you to change to a different one. All the Admin Domains assigned to you are available in the drop-down menu.

For most administrative tasks you must be in either AD0 or the physical fabric. The following procedure describes how to change the Admin Domain. This action is referred to as “changing the Admin Domain context.”

To change the Admin Domain context

1. Select an Admin Domain from the Admin Domain drop-down menu.

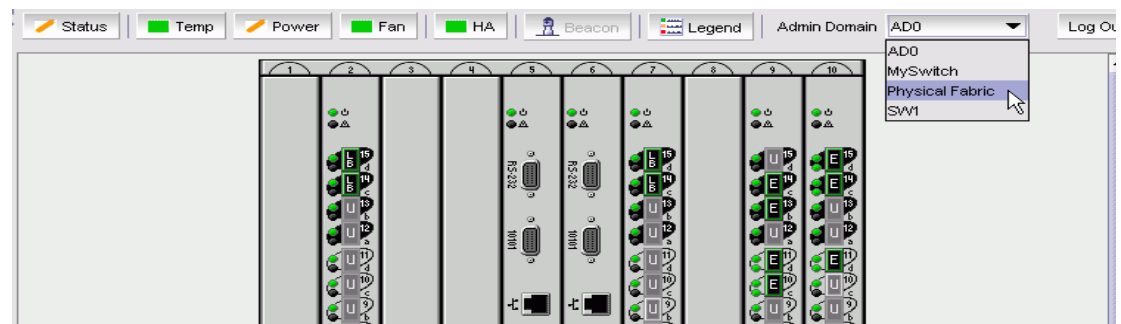


FIGURE 11 Changing the Admin Domain

2. Click **OK** in the confirmation window.

Switch Explorer refreshes to display the new Admin Domain context. A progress bar displays while Switch Explorer is refreshing.

If there are other windows open, the system displays a list of the open windows. You can choose to change the Admin Domain which will close all the open windows, or cancel the action and return to Switch Explorer.

NOTE

The Telnet window, the Fabric Details, and Fabric Events windows are not AD-filtered and do not need to be closed.

SWITCH VIEW BUTTONS

The Switch View buttons let you access the following switch information:

- Status - click the button to view the status of the switch.
- Temperature - click the button to view temperature monitors.
- Power - click the button to view power supply information.
- Fan - click the button to view the status of the switch fans.
- Beaconsing.
- Legend - click the button to view the legend for the Switch View.

NOTE

For all status displays based on errors per time interval, any errors cause the status to show faulty until the entire sample interval has passed.

SWITCH VIEW

The Switch View displays a graphical representation of the selected switch, including a real-time view of switch and port status. Select a switch in the Fabric Tree to access the Switch View for that switch. [Figure 12](#) shows an example of a Switch View.

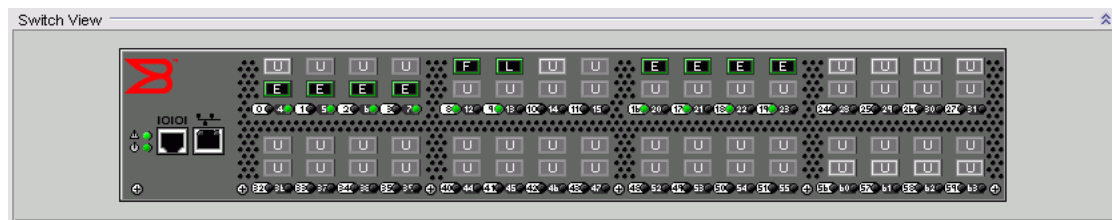


FIGURE 12 Example of a Switch View

Port representations

The ports in the Switch View show the port type. Borders around the accessible ports indicate that SFP modules are present. A colored border indicates the status of the port; for example, a green border indicates that the port is connected and traffic is flowing. For example, in [Figure 12](#), port 20 has a border, 21 does not have a border, and 22 has a colored border. Ports that are not accessible do not display the port type and do not have borders.

The port LEDs in the Switch View match the LEDs on the physical switch; however, the blink rate of the LEDs in the Switch View does not necessarily match the blink rate of the LEDs on the physical switch. See [“Interpreting port LEDs”](#) on page 154 for more information.

Right-click a port in Switch View to get a menu from which you can launch the Port Management module and view detailed information about the port. From Port Management, you can access information on all other ports. See [Chapter 5, “Managing Your Ports”](#) for more information.

If the selected Admin Domain does not include ownership of some ports that are physically present on the switch, these ports are represented as black rectangles with horizontal gray bars indicating they are not accessible. E_Ports are visible in all domains. You cannot launch the Port Management module by clicking these ports. In [Figure 12](#), only ports 16 through 31 (and not the switch) are owned by the current Admin Domain, as shown in the figure:

- E_Ports 0, 1, 14, 24, and 25 are shown as online and accessible.
- All other ports in the range from 0 through 15 are shown as inaccessible, with no type information displayed. If you click the E_Ports in this range, the Port Management module launches in read-only mode.
- Ports in the range from 16 through 31 are both accessible and controllable. When these ports (including E_Ports) are clicked, the Port Management module launches in read-write mode.

Switch View refresh rates

The Switch View display is refreshed at 15 second intervals. However, the initial display of Switch Explorer might take from 30 to 60 seconds after the switch is booted. Refresh rates are fabric-size dependent. The larger the fabric, the longer it takes to poll the fabric and refresh the view. F_Port and L_Port connection changes refresh immediately.

Autorefresh intervals may be not be exactly 15 seconds. The refresh rate varies depending on the activity in the fabric and on the host system you are using.

SWITCH EVENTS AND SWITCH INFORMATION

Switch Events and Switch Information appear as tab forms under Switch View.

Switch Information View displays switch information such as switch name, status, Fabric OS version, domain ID, IP address, WWN, and current zone configuration. The information in the Switch Information View is polled every 60 seconds.

For more information, see [“Displaying switch information”](#) on page 149.

Displaying tool tips

If you hover your cursor most components, the system displays *tool tip* information about the component. [Figure 13](#) shows several examples of tool tips.

In Fabric Tree you can hover over a switch to view its type, Ethernet IP, Fibre Channel IP, and status of the switch.

In Switch View, you can hover over a blade to view the blade ID and its status. It is easier to use the top of the blade to display the tool tip so that you do not inadvertently display the port tool tips.

When you hover over a port, you can view the port number, port index, port type (E, F, L, or U_Port), port status (online or offline), and port state (in-sync, no_sync, no light, or no module). If you right-click the port, the system displays the tool tip information as well as the port world-wide name. For example, [Figure 13](#) displays the mouseover tool tip for port 19 and the right-click tool tip for port 30.

When you hover over the Web Tools buttons, the system displays a brief description of the button.

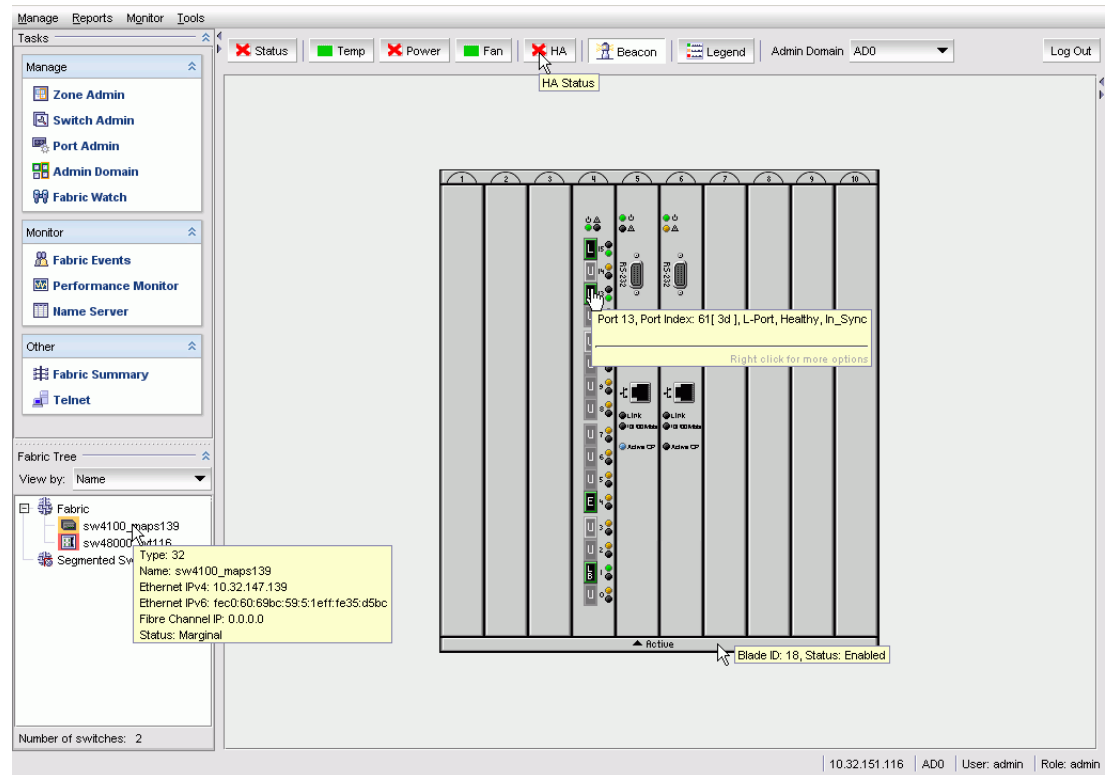


FIGURE 13 Mouseover view of switch information

You can right-click a port to quickly perform some basic port administration tasks, as shown in [Figure 14](#).

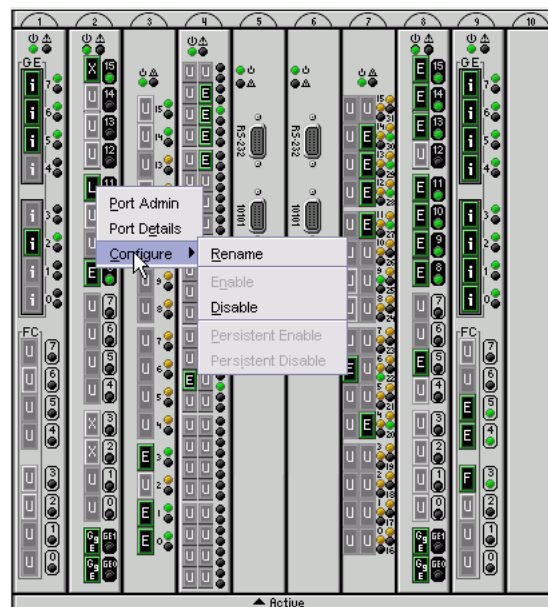


FIGURE 14 Right-click menu for ports (from Switch Explorer)

- The Port Admin option opens the Port Administration window
- The Port Details option displays read-only information about a port, without opening the Port Administration window. You can export and copy the information from the Port Details window.
- The Configure option provides another menu of options to allow you to rename, enable, disable ports, and set persistent enable/disable without opening the Port Administration window.

Refresh rates

Different panels of Web Tools refresh at different rates.

The refresh, or polling, rates listed in this section and throughout the book indicate the time between the end of one polling and the start of the next, and not how often the screen is refreshed. A refresh rate of 15 seconds does not ensure that a refresh occurs every 15 seconds. It ensures that the time between each refresh activity is no more than 15 seconds.

Autorefresh intervals might not be exactly 15 seconds. The refresh rate varies depending on the activity in the fabric and on the host system you are using. Following are some variables you should consider when refreshing the fabric:

- Retrieval time increases when you are in a large fabric as there is more data to fetch from the switch(s).
- Processor speed of the system you are using may slow down the refresh rate.
- OS-Job Scheduling if you are using a host-system in the data center impacts the refresh rate.
- JVM-Performance can contribute to causing interval differences between what is on-screen and how long it is actually taking.

For these reasons, the time displayed in the port statistics tab might not be refreshed as expected. The counter time indicates only that “this statistics data is retrieved from the switch in this time.” To ensure the correct information, the time field is updated along with the port statistics data after every refresh. The lag in refresh rate is more evident in the iSCSI Target Gateway module.

The refresh rates are different for each module. [Table 3](#) lists polling rates by module. Though these rates are sample rates, they correctly illustrate variance in the refresh rates throughout Web Tools.

TABLE 3 Polling rates

Module	Polling Rate
Name Server	User-defined; 15 sec minimum
Zoning Database	60 sec
Fabric Watch	15 sec
Performance Monitor	30 sec
Port Management	2 min
FC Routing	30–90 sec, depending on network traffic

Displaying switches in the fabric

If your fabric has more than one switch, you can launch Web Tools from one switch and then access other switches.

You should not launch switches running Fabric OS v4.4.x or higher from a fabric tree displayed for a pre-v4.4.x switch, as some features might be disabled.

To access Switch Explorer for a particular switch

1. Launch Web Tools as described in [“Launching Web Tools”](#) on page 8 and log in to the switch.
Switch Explorer is displayed for the switch you logged in to.
2. If the Fabric Tree is not expanded, click the plus sign (+) in the Fabric Tree to view all the switches in the fabric.
3. Click a switch in the Fabric Tree.

A separate browser window opens and displays the selected switch. (If the launch switch is running a Fabric OS version earlier than v5.0.1, the selected switch displays in the same browser window.)

The graphic of the selected switch is displayed in the [Switch View](#). Additional switch information is displayed in the [Switch Events](#) and [Switch Information](#).

Using Web Tools and secure mode

When secure mode is enabled on switches you manage through Web Tools, there are requirements and scenarios of which you should be aware. You should read through the requirements and scenarios in this section if you plan to use Web Tools to manage any switches that have secure mode enabled.

WEB TOOLS ACCESS AND HTTP_POLICY

When secure mode is enabled, access to the Web Tools interface is controlled by HTTP_POLICY. If secure mode is enabled and HTTP_POLICY has been defined, your workstation IP address must be included in this policy or you will not have access to Web Tools for any switch in the fabric. If your workstation IP is not included in this policy, the Interface Disabled page is displayed when you attempt to access a switch. For instructions on including your workstation in HTTP_POLICY, see the *Secure Fabric OS Administrator's Guide*.

NOTE

If a secure mode change is made in the fabric—that is, secure mode is enabled, secure mode is disabled, or there is a change to the primary FCS—you must exit and relaunch Web Tools. If Web Tools is kept open after a secure mode change occurs, behavior is undefined.

OPENING MODULES IN A SECURE FABRIC

When opening more than one module in a secure fabric, wait for each module to load completely before opening another. For example, if you want to access both the Zone Admin and the Switch Administration windows, open one of the modules and wait for it to load completely before opening the second module. Abnormal behavior can occur when you attempt to open two modules simultaneously in a fabric with secure mode enabled.

Certain Web Tools features are limited or disabled when secure mode is enabled on a fabric. For more information about secure mode, see the *Secure Fabric OS Administrator's Guide*.

PRIMARY-FCS-ONLY FUNCTIONALITY

The following Web Tools functionality is reserved for the primary FCS when secure mode is enabled:

- Zoning administration is allowed only from the primary FCS switch when secure mode is enabled. For all other switches in a secure fabric, the Zoning button is disabled.
- SNMP community strings can be modified only from the primary FCS switch when secure mode is enabled. For non-FCS switches, you can view the SNMP community strings, but they are read-only, and the SNMP access control lists on the **SNMP** tab are not displayed.
- User account administration is allowed only from the primary FCS switch when secure mode is enabled. The changes are then propagated to all switches in the fabric.

Web Tools provides information about an FCS policy in Switch Explorer. You cannot configure these values from Web Tools, but the Switch Information tab in Switch Explorer provides information as described below:

- If there is no policy distributed, no FCS policy information is displayed.
- If an FCS is distributed, a new section, FC, is displayed on the Switch Information tab in Switch Explorer. The new section shows the values for 2 FCS-related parameters:
 - FCS Enabled (yes or no, but will always be yes if the parameter is visible)
 - FCS Primary Switch (yes or no)
- If FCS is enabled and the switch is not primary, the following restrictions are enforced:
 - Zone Administration and Admin Domain windows are read only.
 - ACL policies can be created and edited locally but not saved.
 - ACL distribution is disabled.

DISABLED FUNCTIONALITY

Telnet access to a switch and the Telnet button in Web Tools are both disabled when secure mode is enabled for a fabric. You must use sectelnet or SSH to access the Fabric OS CLI in a secure fabric. These capabilities are not accessible from Web Tools. For more information on sectelnet or SSH, see the *Secure Fabric OS Administrator's Guide*.

The SNMP Access Control List is replaced with RSNMP_POLICY and WSNMP_POLICY when secure mode is enabled for a fabric. The SNMP Access Control List is not displayed in Web Tools.

Working with Web Tools: recommendations

This section lists recommendations for working with Web Tools:

- If you receive an error when saving changes in the Switch Administration window, note the error messages, refresh the window, and make your changes again. Do not continue making changes without refreshing the window and determining which changes were saved correctly.
- In a mixed fabric—that is a fabric containing switches and directors running v5.x, v4.x, v3.x, and v2.x firmware—use the most advanced switches or directors to control the fabric. For example, use the v5.2.0 switches or directors as the primary FCS, the location to perform zoning tasks, and the time server (CLI). You should use the most recently released firmware on your switches.

- If switches are accessed simultaneously from different connections (for example, Web Tools, CLI, and API), changes from one connection might not be updated to the other, and some modifications might be lost. Make sure that, when you connect with simultaneous multiple connections, you do not overwrite the work of another connection.
- Several tasks in Web Tools make fabric-level changes: for example, the tasks in the Zone Admin module. When executing fabric-level configuration tasks, wait until you have received confirmation that the changes are implemented before executing any subsequent tasks. For a large fabric, this can be up to a few minutes.
- Some data collection and processing operations in the iSCSI Gateway module might take a long time to complete, especially in large fabrics or fabrics with large numbers of Discovery Domains and Discovery Domain Sets defined. In most cases, progress bars are provided. Allow the application a sufficient amount of time (30-40 seconds) to collect and display data before taking any action or assuming the application is “hanging.”
- A maximum of five simultaneous HTTP sessions to any one switch is recommended. An HTTP session is considered a Fabric Manager or Web Tools connection to the switch.

2 Working with Web Tools: recommendations

Managing Fabrics and Switches

In this chapter

This chapter contains the following sections:

- Managing fabrics and switches using Web Tools . . . 29
- Opening the telnet window. 31
- Configuring IP and netmask information 32
- Configuring a syslog IP address. 33
- Managing blades 34
- Configuring a switch 37
- Rebooting the switch 39
- Changing system configuration parameters. 39
- Managing licensed features. 43
- Administering High Availability. 45
- Monitoring events 48
- Displaying a fabric summary report 53
- Displaying the Name Server entries 53
- Physically locating a switch using beaconing. 55

Managing fabrics and switches using Web Tools

You can perform most of the management tasks described in this chapter through the Switch Administration window. Information in the Switch Administration window is retrieved from the selected switch.

Click **Switch Admin** in the **Manage** section of the **Tasks** menu to access the Switch Administration window. [Figure 15](#) on page 30 shows the Switch Administration window.

3 Managing fabrics and switches using Web Tools

If the switch is not a member of the selected Admin Domain, most tabs in the Switch Administration window display in read-only mode, regardless of what permission level you have. The User tab is editable because most of the information on it does not require switch membership in the current Admin Domain.

Switch Administration window, Switch tab

SwitchName: sw48000_wt116 DomainID: 1 VVWN: 10:00:00:60:69:e4:24:e0 Tue Apr 17 2007 18:45:28 GMT+00:00

Switch Network Firmware Download License User Blade Trunking

Name and ID

Name: sw48000_wt116 Manufacturer Serial #: QV060000088

Domain ID: 1 Supplier Serial #: none

Switch Status

☒ Enable ☐ Disable

DNS Configuration

DNS Server 1: fec0:60:69bc:59:60:69ff:fee4:1246

DNS Server 2: fec0:60:69bc:59:60:69ff:fee4:1246

Domain Name: abc.com

Remove All

Report

View Report

Reboot/Fastboot

Reboot Fastboot

Apply Close Refresh

[Switch Administration opened]: Tue Apr 17 2007 17:59:07 GMT+00:00

Change current switch settings Mode: Basic 10.32.151.116 AD0 User: admin Role: admin

FIGURE 15 Switch Administration window, Switch tab

With the exception of switch time, information displayed in the Switch Administration window is *not updated automatically* by Web Tools. To update the information displayed in the Switch Administration window, see [“Refreshing the Switch Administration window”](#) on page 31.

ATTENTION

Most changes you make in the Switch Administration window are buffered, and are *not* applied to the switch until you save the changes. If you close the Switch Administration window without saving your changes, your changes are lost. To save the buffered changes you make in the Switch Administration window to the switch, click **Apply** before closing the module or before switching to another tab. The **License** tab is an exception. Any changes you make on the **License** tab are applied immediately and there is no **Apply** button.

Some of the management tasks for the Brocade 24000 and 48000 directors are performed through the High Availability window. This module and the associated tasks are described in [“Administering High Availability”](#) on page 45.

You can also use telnet commands to perform management tasks. See [“Opening the telnet window”](#) on page 31 for information on how to launch a telnet window using Web Tools.

The remainder of this section describes basic Switch Administration window procedures that are useful for many switch management operations.

OPENING THE SWITCH ADMINISTRATION WINDOW

Most of the management procedures in this chapter are performed from the Switch Administration window.

To open the Switch Administration window

1. Select a switch in [Fabric Tree](#).

The switch is displayed in Switch View.

2. Click **Switch Admin** in the **Manage** section of the **Tasks** menu.

The Switch Administration window opens in basic mode, as shown in [Figure 15](#) on page 30. The basic mode displays the “basic” tabs and options.

3. To see all the tabs and options, click the Show Advanced Mode button.

REFRESHING THE SWITCH ADMINISTRATION WINDOW

You can refresh the fabric element information displayed at any time using the following procedure. Note that when you click a different tab in the Switch Administration window, the information in the newly selected tab is automatically refreshed.

To refresh the fabric information

1. Click the **Refresh** button on any tabbed page of the Switch Administration window.

Opening the telnet window

When you open a telnet window, the connection is to the IP interface of the switch. For each switch, you must open a telnet window.

You cannot connect to CP blades that do not have separate IP addresses. Also, you cannot connect using Web Tools to a CP blade on a director switch even when the blade has an IP address and supports telnet sessions. See the *Fabric OS Command Reference* for information about the telnet commands.

NOTE

Telnet access to a switch and the **Telnet** button in Web Tools are both disabled when secure mode is enabled for a fabric. You must use **sectelnet** or **SSH** to access the Fabric OS command line interface in a secure fabric. These capabilities are not accessible from Web Tools. For more information on sectelnet or SSH, see the *Secure Fabric OS Administrator's Guide*.

Internet Explorer 7.0 default settings disable telnet functionality. If you are using Internet Explorer 7.0, you must make the appropriate changes in the registry to open the telnet window.

3 Configuring IP and netmask information

To access telnet through Web Tools

1. Select a switch in [Fabric Tree](#).

You are prompted to log in if the OS is version 5.3.0. Otherwise, the selected switch appears in the [Switch View](#).

2. Click the **Telnet** button in the **Other** section of the **Tasks** menu.

Web Tools opens two windows: the Telnet window and another HTML-based window which is used to launch the Telnet window. Click OK to close the HTML-based window. The Telnet window remains open.

3. In the telnet window, enter your user credentials at the login prompt.
4. To close the session, type **exit** at the prompt.

Configuring IP and netmask information

When you configure IP and netmask information for the Brocade 24000 or 48000 director, you must configure IP and subnet mask information individually.

When you change the Ethernet IP, subnet mask, gateway IP, or Fibre Channel IP and subnet mask from Web Tools, there is a normal loss of network connection to the switch. If the IP properties have changed, you must close all current windows and restart Web Tools with the new IP address.

To configure IP and netmask information

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **Network** tab.

SwitchName: WT_111_Saturn DomainID: 111 VVWV: 10:00:00:05:1e:36:01:90 Fri May 25 2007 15:07:11 GMT+00:00

Switch Network Firmware Download License User Blade Trunking

IPv4 Address

Ethernet IP: 10.33.13.111 Fibre Channel Net IP: 0.0.0.0

Ethernet Mask: 255.255.240.0 Fibre Channel Net Mask: 0.0.0.0

Gateway IP: 10.33.0.1 DHCP: Disabled

IPv6 Address

Ethernet IPv6: /

Advanced IP Configuration

IPv4 Address

CP0 Ethernet IPv4: 10.33.13.112 CP1 Ethernet IPv4: 10.33.13.113

CP0 IPv4 Subnet Mask: 255.255.240.0 CP1 IPv4 Subnet Mask: 255.255.240.0

IPv6 Address

CP0 Ethernet IPv6: / CP1 Ethernet IPv6: /

Syslog IP's Configuration

Items: 5

Syslog IP	Current Value
1	10.32.159.49
2	10.33.8.19
3	10.33.8.159
4	10.33.7.19
5	10.33.3.3


New IP: Add Remove Clear All

Apply Close Refresh

FIGURE 16 Network tab

3. In the appropriate IP Address section, enter an IP address (for example, 10.77.77.77).
Use the IPv4 Address section and/or the IPv6 Address section to specify IP addresses.
4. For the Brocade 24000 and 48000 directors only:

In the Advanced Configuration area, type valid IP addresses for the Ethernet IP and subnet mask for CPO and CP1.

If the Advanced Configuration area is not visible, click the expand arrows  on the right, to expand the area.
5. Click **Apply**.
6. Click **Close** to exit, and then restart Web Tools to continue working.

Configuring a syslog IP address

The syslog IP represents the IP address of the server that is running the syslog process. The syslog daemon reads and forwards system messages to the appropriate log files and/or users, depending on the system configuration. When one or more IP addresses are configured, the switch forwards all error log entries to the syslog on the specified servers. Up to six servers are supported. See *Fabric OS Administrator's Guide* for more information on configuring the syslog daemon.

When you configure a syslog IP address for a Brocade 24000 configured with two logical switches, it is on a logical-switch basis. This means that for each logical switch, you must configure a syslog IP address individually.

To configure the syslog IP address

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **Network** tab (see [Figure 16](#)).
3. In the **New IP** field, enter an IP address in either IPv4 or IPv6 format, or enter a DNS name.
4. Click **Add**.

The new IP address is displayed in the Syslog IP area.
5. Click **Apply**.

To remove a syslog IP address

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **Network** tab.
3. Select a syslog IP in the table and click **Remove**.

You can click **Clear All** to remove all of the syslog IP addresses from the table.
4. Click **Apply**.

Filtering IP Addresses

Web Tools provides the ability to control what client IP addresses may connect to a switch or fabric

To set up IP filtering

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **IP Filtering** tab.

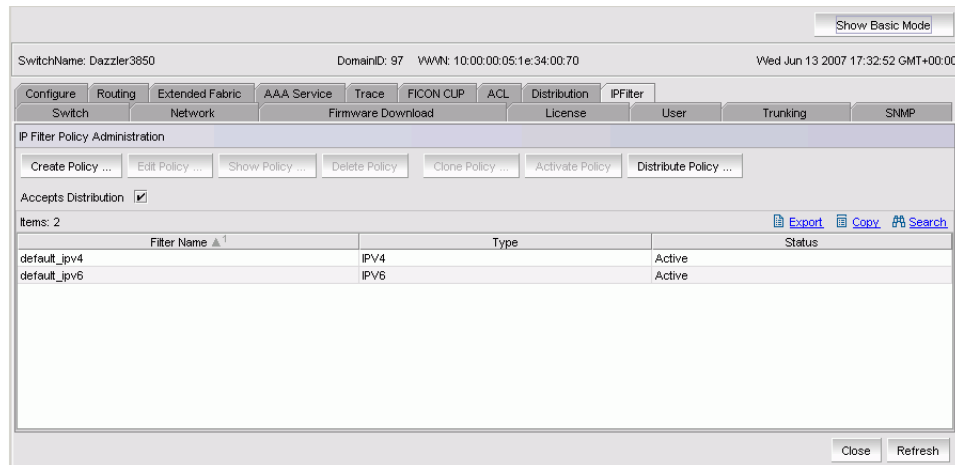


FIGURE 17 IP Filter tab

3. Click **Create Policy**.
The Create IP Filter Policy window opens.
4. Enter a policy name, choose a policy type, and then click the **Add Rule** button.
5. Enter the rule order and source IP address, and modify the service/destination port, protocol, and action as necessary.
6. Click **OK**.

After you create a policy, you can use the other buttons on this tab to manage the policies:

- **Edit Policy** lets you select an existing policy and make changes to it.
- **Show Policy** lets you view the details of the policy in a read-only window.
- **Delete Policy** lets you delete a policy.
- **Clone Policy** lets you copy a policy. Use this feature when you want to create similar policies. After you create a clone, you can edit the policy to make the appropriate changes.
- **Activate Policy** lets you make an existing policy active.
- **Distribute Policy** lets you distribute a policy to various switches.

Managing blades

Web Tools provides the ability to enable and disable blades, and to set slot-level IP addresses for blades. The procedure in this section applies only to the Brocade 24000 and 48000 directors (bladed switches).

ENABLE OR DISABLE A BLADE

To enable or disable a blade

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **Blade** tab.

The Firmware Version columns display the firmware loaded onto each blade. A blade can have more than one firmware image loaded onto it.

The Enable Blade column in the Blade tab pane indicates whether the blade is enabled.

SwitchName: sw48000_wt124 DomainID: 124 VVNT: 10:00:00:05:1e:36:0c:7a lun. mai 21 2007 05:46:29 GMT+00:00

Switch Network Firmware Download License User **Blade** Trunking

Set IP Address... Show IP Address...

Blade Administration

Items: 10 Export Copy Search

Slot No	Blade Id	Blade Type	Firmware Version		Blade State	Enable Blade
			Primary	Secondary		
1		UNKNOWN	N/A	N/A	ABSENT	<input type="checkbox"/>
2	17	SW_BLADE	N/A	N/A	ENABLED	<input checked="" type="checkbox"/>
3	33(FA4-18)	AP_BLADE	(FOS) 5.3.0_rel_bld43 (SAS) 3.0.0_ssr_bld28 (DMM) 3.0.0_scimitar_bld08	(FOS) 5.3.0_rel_bld43 (SAS) 3.0.0_ssr_bld28 (DMM) 3.0.0_scimitar_bld08	ENABLED	<input checked="" type="checkbox"/>
4		UNKNOWN	N/A	N/A	ABSENT	<input type="checkbox"/>
5	16	CP_BLADE	5.3.0_rel_bld43	5.3.0_rel_bld43	STANDBY	<input type="checkbox"/>
6	16	CP_BLADE	5.3.0_rel_bld43	5.3.0_rel_bld43	ACTIVE	<input type="checkbox"/>
7		UNKNOWN	N/A	N/A	ABSENT	<input type="checkbox"/>
8		UNKNOWN	N/A	N/A	ABSENT	<input type="checkbox"/>
9		UNKNOWN	N/A	N/A	ABSENT	<input type="checkbox"/>
10		UNKNOWN	N/A	N/A	ABSENT	<input type="checkbox"/>

Apply Close Refresh

[Switch Administration opened]: lun. mai 21 2007 05:32:37 GMT+00:00

Set IP address for two Ethernet interfaces Mode: Basic 10.32.151.124 AD0 User: root Role: root

FIGURE 18 Blade tab

3. Select the **Enable Blade** check box for each blade you want to enable. Clear the check box to disable the blade. You cannot enable or disable the CP blades.
4. Click **Apply**.

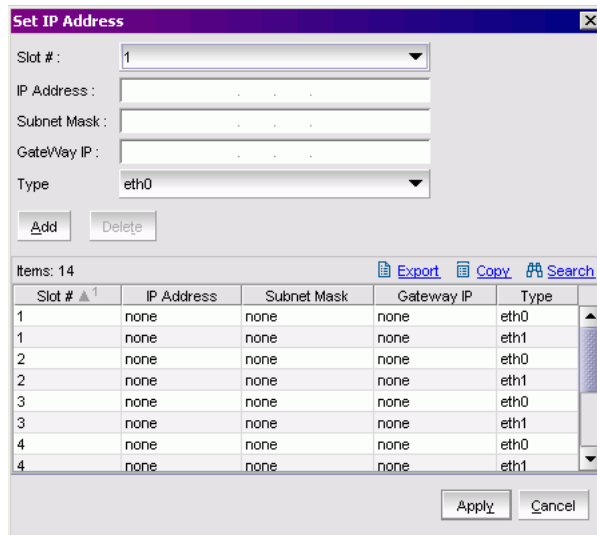
Set IP address

To set a slot-level IP address

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **Blade** tab.

3 Managing blades

3. Click the Set IP address button.



The 'Set IP Address' dialog box contains the following fields and controls:

- Slot #: A drop-down menu with '1' selected.
- IP Address: A text input field.
- Subnet Mask: A text input field.
- GateWay IP: A text input field.
- Type: A drop-down menu with 'eth0' selected.
- Buttons: 'Add' and 'Delete'.
- Table: A table with 5 columns: Slot #, IP Address, Subnet Mask, Gateway IP, and Type. It contains 8 rows of data, all with 'none' for IP, Subnet Mask, and Gateway IP, and either 'eth0' or 'eth1' for Type.
- Buttons: 'Apply' and 'Cancel'.

Slot #	IP Address	Subnet Mask	Gateway IP	Type
1	none	none	none	eth0
1	none	none	none	eth1
2	none	none	none	eth0
2	none	none	none	eth1
3	none	none	none	eth0
3	none	none	none	eth1
4	none	none	none	eth0
4	none	none	none	eth1

FIGURE 19 Set IP Address dialog box

4. Select a slot number from the drop-down list.
5. Enter the IP address, subnet mask, and Gateway IP address.
6. Select a type from the drop-down list.
7. Click Add to add the new entry to the table.

When you click the Add button, the values remain in the fields.

8. To delete a configuration, select a row in the table and click the Delete button.

NOTE

Clicking the Add or Delete buttons update the table in the Set IP Address dialog box, but does not send values to the switch.

9. Click the Apply button to save the values currently shown in the table to the switch or click Cancel to close the dialog box without saving any of your changes.

To update the switch with you changes, you must update the table using the Add and Delete buttons, and then click Apply.

View IP addresses

If you want to view the IP addresses configured on the switch for the currently populated slots, use the Show IP Address button.

To view the IP addresses

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **Blade** tab.

3. Click the Show IP Address button.

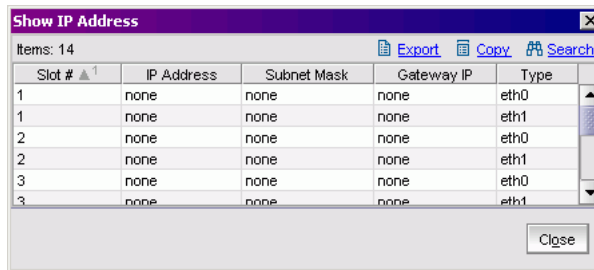




FIGURE 20 Show IP Address dialog box

4. Scroll through the list to view all the information.
5. When you are done, click Close.

Configuring a switch

Use the **Switch** tab of the Switch Administration window to perform basic switch configuration. [Figure 15](#) on page 30 shows an example of the **Switch** tab.

ENABLING AND DISABLING A SWITCH

You can identify if a switch is enabled or disabled in the Switch Administration window by looking at the lower-right corner: the  icon means that the switch is enabled, and the  icon means that the switch is disabled. If you hover the cursor over the icon, the system displays text that indicates the status of the switch.

To enable or disable a switch

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **Switch** tab.
3. Click the **Enable** radio button in the **Switch Status** section to enable the switch, or click the **Disable** radio button to disable the switch.
4. Click **Apply**.

The system displays a confirmation window that asks if you want to save the changes to the switch. You must click **Yes** to save the changes.

CHANGING THE SWITCH NAME

Switches can be identified by IP address, domain ID, World Wide Name (WWN), or customized switch names that are unique and meaningful.

Switch names can be a maximum of 15 characters for Fabric OS v5.3.0. Names must begin with an alphabetic character, but otherwise can consist of alphanumeric and underscore characters.

NOTE

It is recommended that you customize the chassis name for each switch. Some system messages identify a switch service by the chassis name, so if you assign meaningful chassis names in addition to meaningful switch names, logs will be more useful. You change the chassis name using the CLI. See the *Fabric OS Administrator's Guide* for instructions on changing the chassis name.

To change the switch name

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **Switch** tab.
3. Type a new name in the **Name** field and click **Apply**.

CHANGING THE SWITCH DOMAIN ID

Although domain IDs are assigned dynamically when a switch is enabled, you can request a specific ID to resolve a domain ID conflict when you merge fabrics.

To change the switch domain ID

1. Open the Switch Administration window as described on [page 31](#).
2. Disable the switch, as described in [“Enabling and disabling a switch”](#) on page 37.
3. Click the **Switch** tab.
4. Type a new domain ID in the **Domain ID** field.
The domain ID is an integer between 1 and 239.
5. Click **Apply**.
6. Enable the switch, as described in [“Enabling and disabling a switch”](#) on page 37.

VIEWING AND PRINTING A SWITCH REPORT

The switch report includes the following information:

- A list of switches in the fabric
- Switch configuration parameters
- A list of ISLs and ports
- Name Server information
- Zoning information
- SFP serial ID information

To view or print a switch report

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **Switch** tab.
3. Click **View Report**.
4. In the new window that displays the report, view or print the report using your browser.

Rebooting the switch

When you reboot the switch, the reboot takes effect immediately. Ensure that there is no traffic or other management on the switch, as traffic is interrupted during the reboot; however, frames are not dropped. Be sure to save your changes before the reboot, as any changes that were not saved are lost.

PERFORMING A FAST BOOT

A fast boot reduces boot time significantly by bypassing the power-on self test (POST).

To perform a switch fast boot

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **Fastboot** button.
3. On the Fastboot Confirmation window, click Yes to continue.
4. Click **Apply**.

PERFORMING A REBOOT

Use the following procedure to reboot the CP and execute the normal power-on booting sequence.

To perform a switch reboot

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **Reboot** button.
3. On the Reboot Confirmation window, click Yes to continue.
4. Click **Apply**.

Changing system configuration parameters

When you change system configuration parameters for a Brocade 24000 configured with two logical switches, it is on a logical-switch basis. This means that for each logical switch, you must change the system configuration parameters individually.

You must disable the switch before you can configure fabric parameters.

You can change the following system configuration parameters:

- Switch fabric settings
- Virtual channel settings
- Arbitrated loop parameters
- System services

CONFIGURING FABRIC PARAMETERS

To configure the following fabric parameters, click the **Show Advanced Mode** button of the Switch Administration window, and use the **Configure** tab and **Fabric** subtab (as shown in [Figure 21](#) on page 41):

3 Changing system configuration parameters

- **BB Credit**

The buffer-to-buffer credit is the number of buffers available to attached devices for frame receipt. The default BB Credit is 16. The range is 1–27.
- **R_A_TOV**

Resource allocation timeout value (in milliseconds). This variable works with the E_D_TOV to determine switch actions when presented with an error condition. The default is 10000. The possible range is 4000–120000.
- **E_D_TOV**

Error detect timeout value (in milliseconds). This timer is used to flag a potential error condition when an expected response is not received within the set time. The valid range is 1000–5000.
- **Datafield size**

The largest possible data field size (in bytes). The valid range is 256–2112.
- **Switch PID Format**

Select a switch PID format from one of the following:

 - Format 1 (0-base, 256 encoding)
 - Format 2 (16-base, 256 encoding)
- **Sequence Level Switching**

Select this box to enable frames of the same sequence from a particular group to be transmitted together. When this option is not selected, frames are transmitted interleaved among multiple sequences. Under normal circumstances, sequence-level switching should be disabled for better performance. However, some host adapters have issues when receiving interleaved frames among multiple sequences.
- **Disable Device Probing**

Set this mode only if the switch N_Port discovery process (PLOGI, PRLI, INQUIRY) causes an attached device to fail. When set, devices that do not register with the Name Server are not present in the Name Server database.
- **Per-Frame Routing Priority**

Choose whether to select per-frame routing priority. When enabled, the virtual channel ID is used in conjunction with a frame header to form the final virtual channel ID.
- **Suppress Class F Traffic**

Applies only if VC-encoded address mode is also set. When selected, translatable addressing (which allows private devices to communicate with public devices) is disabled.
- **Insistent Domain ID Mode**

Set this mode to make the current domain ID insistent across reboots, power cycles, and failovers. This mode is required fabric wide to transmit FICON data.

SwitchName: sw48000_wt116 DomainID: 1 WWN: 10:00:00:60:69:e4:24:e0 Tue Apr 17 2007 19:32:05 GMT+00:00

Routing Extended Fabric AAA Service Trace FICON CUP ACL Distribution IPFilter IPsec Policies
Switch Network Firmware Download License User Blade Trunking SNMP Configure

BB Credit 1 ☐ Sequence Level Switching
R_A_TOV 4000 ☐ Disable Device Probing
E_D_TOV 1000 ☐ Per-Frame Routing Priority
Datafield Size 256 ☐ Suppress Class F Traffic
Switch PID Format Format 1 (0-base, 256 port Encoding) ☐ Insistent Domain ID Mode

Fabric Virtual Channel Arbitrated Loop System Upload/Download

Apply Close Refresh

[Switch Administration opened]: Tue Apr 17 2007 19:09:43 GMT+00:00

Configure Switch Parameters Mode: Advanced 10.32.151.116 AD0 User: admin Role: admin

FIGURE 21 Configure tab, Fabric subtab

To configure fabric parameters

1. Open the Switch Administration window as described on [page 31](#).
2. Disable the switch as described in “[Enabling and disabling a switch](#)” on page 37.
3. Click the **Configure** tab.
4. Click the **Fabric** subtab.
5. Make the fabric parameter configuration changes.
6. Click **Apply**.
7. Enable the switch as described in “[Enabling and disabling a switch](#)” on page 37.

ENABLING INSISTENT DOMAIN ID MODE

When insistent domain ID (ID_ID) mode is enabled, the current domain setting for the switch is insistent; that is, the same ID is requested during switch reboots, power cycles, CP failovers, firmware downloads, and fabric reconfigurations. If the fabric does not assign the insistent domain ID, the switch segments from the fabric.

To enable insistent domain ID mode

1. Open the Switch Administration window as described on [page 31](#).
2. Disable the switch as described in “[Enabling and disabling a switch](#)” on page 37.
3. Click the **Configure** tab.
4. Click the **Fabric** subtab.
5. Select the **Insistent Domain ID Mode** check box.
6. Click **Apply**.
7. Enable the switch as described in “[Enabling and disabling a switch](#)” on page 37.

CONFIGURING VIRTUAL CHANNEL SETTINGS

You can configure parameters for eight virtual channels (VC) to enable fine-tuning for a specific application. You cannot modify the first two virtual channels, which are reserved for switch internal functions.

ATTENTION

The default virtual channel settings have already been optimized for switch performance. Changing the default values can improve switch performance but can also degrade performance. Do not change these settings without fully understanding the effects of the changes.

VC Priority specifies the class of frame traffic given priority for a virtual channel.

To configure system services

1. Open the Switch Administration window as described on [page 31](#).
2. Disable the switch as described on [page 37](#).
3. Click the **Configure** tab.
4. Click the **Virtual Channel** subtab.
5. Type a value in the VC Priority field you want to change. Valid values for all fields are 2 or 3.
6. Click **Apply**.
7. Enable the switch as described on [page 37](#).

CONFIGURING ARBITRATED LOOP PARAMETERS

You can configure the following arbitrated loop parameters using the **Configure** tab and **Arbitrated Loop** subtab of the Switch Administration window:

- | | |
|-------------------------|--|
| Send Fan Frames | Select this check box to specify that fabric address notification (FAN) frames are sent to public loop devices to notify them of their node ID and address. |
| Always Send RSCN | Following the completion of loop initialization, a remote state change notification (RSCN) is issued when FL_Ports detect the presence of new devices or the absence of pre-existing devices. Select this check box to issue an RSCN upon completion of loop initialization, regardless of the presence or absence of new or pre-existing devices. |
| Do Not Allow AL_PA 0x00 | Select this box to disable 0x00 as an AL_PA value. |

To configure arbitrated loop parameters

1. Open the Switch Administration window as described on [page 31](#).
2. Disable the switch as described in “[Enabling and disabling a switch](#)” on page 37.
3. Select the **Configure** tab.
4. Select the **Arbitrated Loop** subtab.
5. Select or clear the check boxes to enable or disable the corresponding arbitrated loop parameters.
6. Click **Apply**.
7. Enable the switch as described in “[Enabling and disabling a switch](#)” on page 37.

CONFIGURING SYSTEM SERVICES

You can enable or disable FCP read link status (RLS) probing for F_Ports and FL_Ports. It is disabled by default.

To configure system services

1. Open the Switch Administration window as described on [page 31](#).
2. Disable the switch as described in “[Enabling and disabling a switch](#)” on page 37.
3. Click the **Configure** tab and click the **System** subtab.
4. Select the **Disable RLS Probing** check box to *disable* RLS probing. Clear the check box to *enable* RLS probing.
5. Click **Apply**.
6. Enable the switch as described in “[Enabling and disabling a switch](#)” on page 37.

Managing licensed features

Feature licenses might be supplied with switch software, or you can purchase licenses separately from your switch vendor, who will provide you with keys to unlock the features. License keys are provided on a per-chassis basis, so for products that support multiple logical switches (domains), a license key applies to all domains within the chassis.

3 Managing licensed features

The licensed features currently installed on the switch are listed in the **License** tab of the Switch Administration window, as shown in [Figure 22](#). If the feature is listed, it is installed and immediately available. When you enable some licenses, such as ISL Trunking, you might need to change the state of the port to enable the feature on the link.

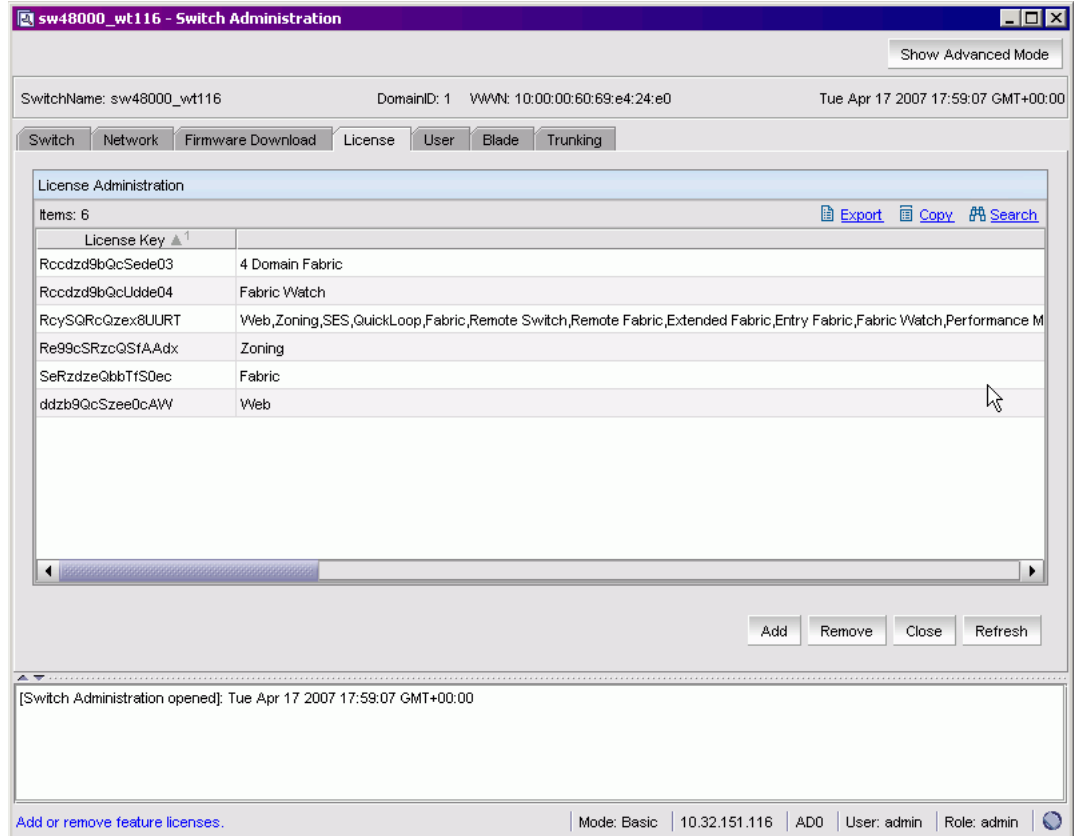


FIGURE 22 License tab

Use the links above the table to export data, copy data, or search the table.

ACTIVATING A LICENSE ON A SWITCH

Before you can unlock a licensed feature, you must obtain a license key. You can either use the license key provided in the paperpack document supplied with switch software or see the *Fabric OS Administrator's Guide* for instructions on how to obtain a license key at the Brocade Web site (www.brocade.com).

NOTE

Some licenses (for example, Trunking) do not take effect until the switch is rebooted.

To activate a license on a switch

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **License** tab and click **Add**.

The Add License dialog box displays.

3. Paste or type a license key in the field.
4. Click **Add License**.
5. Click **Refresh** to display the new licenses in the **License** tab.

REMOVING A LICENSE FROM A SWITCH

You can remove a license from a switch in the Switch Administration window.

ATTENTION

Use care when removing licenses. If you remove a license for a feature, that feature will no longer work. Removing the Web Tools license from a switch makes that switch unavailable from Web Tools.

To remove a license from a switch

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **License** tab.
3. Click the license you want to remove.
4. Click **Remove**.

Administering High Availability

High-Availability (HA) features provide maximum reliability and nondisruptive replacement of key hardware and software modules.

The procedures in this section apply only to the Brocade 24000 and 48000 directors, because the High Availability module is available only on these switch types. See the *Fabric OS Administrator's Guide* for additional information about High Availability.

The High Availability module (see [Figure 23](#) on page 46) displays information about the status of the HA feature on the Brocade 24000 and 48000 directors and each CP, and enables you to perform CP failover.

The background color of the HA button indicates the overall status of high availability on the switch. The colors and their meanings are as follows:

- **Green**—Healthy: HA Status is “Non-Disruptive Failover Ready”
- **Yellow**—Disruptive mode HA Status is “Disruptive Failover Ready”
- **Red**—HA is unavailable: HA Status is “Non-Redundant”

Admin Domain considerations: HA is possible if the switch is a member of the current Admin Domain. If switch is not a member of current Admin Domain, **Synchronize Services** and **Initiate Failover** buttons will be unavailable.

LAUNCHING THE HIGH AVAILABILITY MODULE

Admin Domain considerations: To launch the High Availability window, the switch has to be a member of the Admin Domain you are currently logged in to. If the switch is *not* a member of the current Admin Domain, **Synchronized Services** and **Initiate Failover** will be disabled.

To launch the High Availability window

1. Select a Brocade 24000 or 48000 director from the [Fabric Tree](#).

The selected director appears in the [Switch View](#).

2. Click the **HA** button in the [Switch View](#).

The **High Availability** window opens.

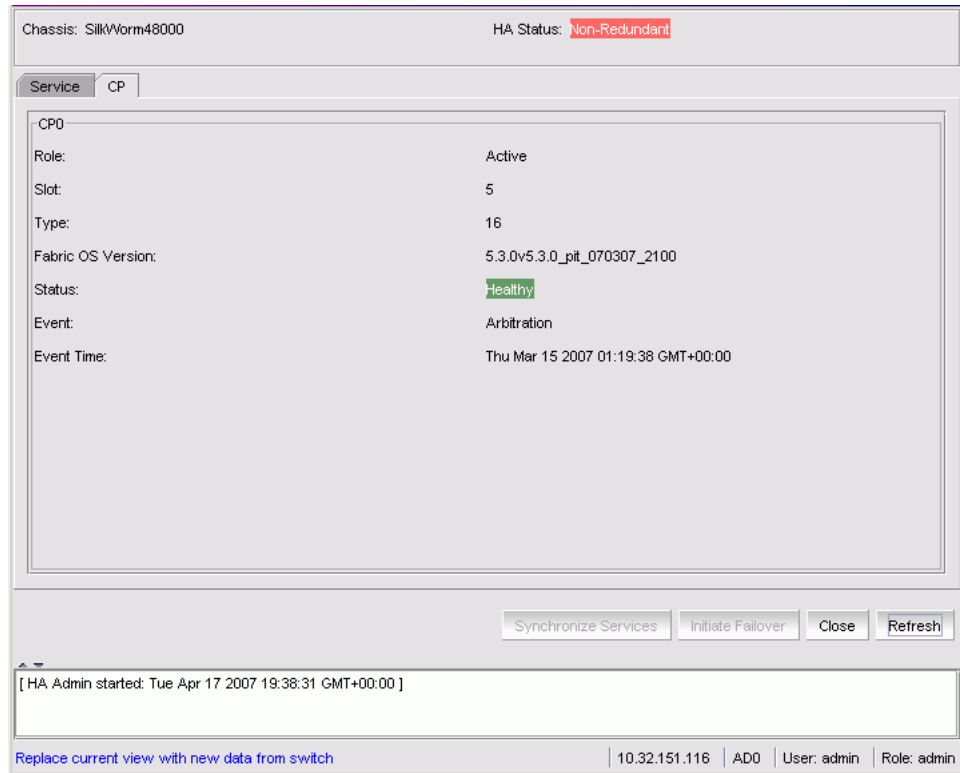


FIGURE 23 High Availability window, CP tab

Note that the highlight color of the HA Status at the top of the module is the same as the background color of the **HA** button.

The High Availability window contains two tabs:

- The **Service** tab displays information about the switch. When the hardware is configured as a dual switch, the **Service** tab displays information about both switches.
- The **CP** tab displays information about slot 5 and slot 6.

In the **Service** tab, you can click the **Detail** button for the standby CP to get additional status.

The High Availability window is not refreshed automatically. Click **Refresh** to update the information displayed in the High Availability window.

SYNCHRONIZING SERVICES ON THE CP

A nondisruptive CP failover is only possible when *all* the services have been synchronized between both CPs.

To synchronize the services

1. Open the High Availability window as described in “[Launching the High Availability Module](#)” on page 45.
2. Verify that HA Summary field displays Non-Disruptive Failover Ready.
If the HA Status field displays **Non-Disruptive Failover Ready**, you are done.
If the HA Status field displays **Disruptive Failover Ready**, continue with step 3.
3. Click the **Synchronize Services** button.
The Warning dialog box displays.
4. Click **Yes** and wait for the CPs to complete a synchronization of services, so that a nondisruptive failover is ready.
5. Click **Refresh** to update the HA Status field.

When the HA Status field displays **Non-Disruptive Failover Ready**, a failover can be initiated without disrupting frame traffic on the fabric.

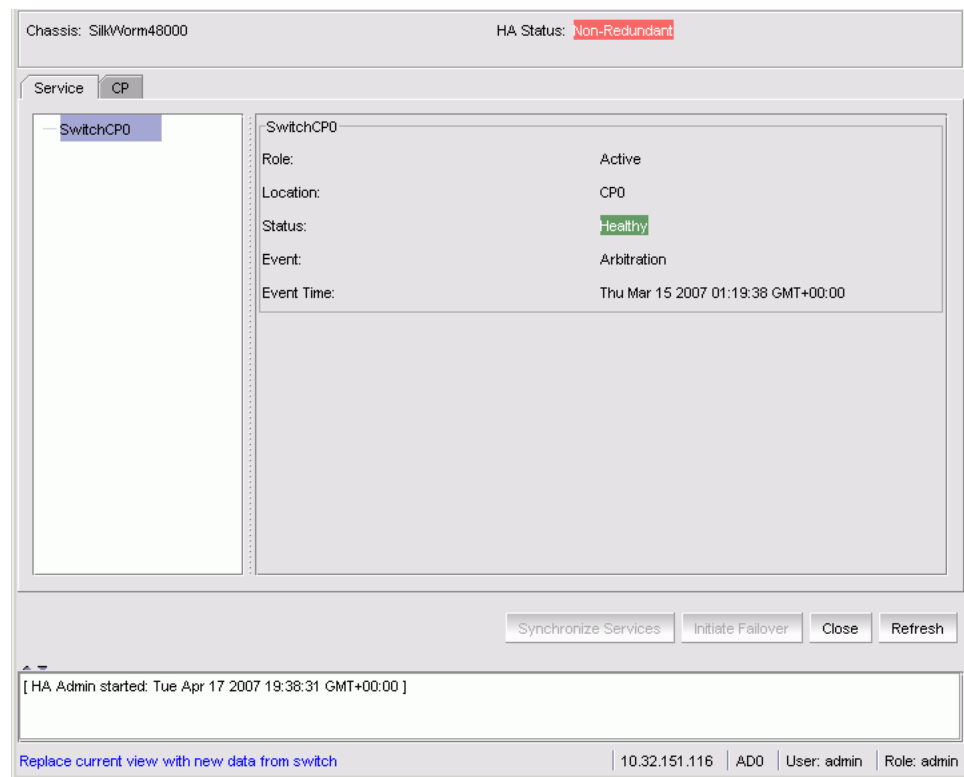


FIGURE 24 High Availability window, Services tab

INITIATING A CP FAILOVER

A nondisruptive failover might take about 30 seconds to complete. During the failover, all of the Web Tools windows and all associated child-windows are invalidated. You must close all Web Tools windows and relaunch Web Tools.

To initiate a CP failover

1. Open the High Availability window as described in [“Launching the High Availability Module”](#) on page 45.
2. Verify that the HA Status field displays **Non-Disruptive Failover Ready** or **Disruptive Failover Ready**.
3. Click **Initiate Failover**.
The Warning dialog box displays.
4. Click **Yes** to initiate a nondisruptive failover.
5. When prompted, close the Web Tools Switch Explorer window and all associated windows, and relaunch Web Tools.

Monitoring events

Web Tools displays fabric-wide and switch-wide events. Event information includes sortable fields for the following:

- Switch name
- Message number
- Time stamp
- Indication of whether the event is from a logical switch or a chassis
- The number of successive events of the same kind
- Severity level
- Unique message identifier (in the form *moduleID-messageType*)
- Detailed error message for root cause analysis

There are four message severity levels: Critical, Error, Warning, and Info. [Table 4](#) lists the event message severity levels displayed on the Switch Events tab and in the Fabric Events window, and explains what qualifies event messages to be certain levels.

On the Switch Events tab and in the Fabric Events window, you can click the **Filter** button to launch the Filter Events dialog box. The Filter Events dialog box allows you to define which events should be displayed on the Switch Events tab or in the Fabric Events window. For more information on filtering events, see [“Filtering Fabric and Switch Events”](#) on page 51.

TABLE 4 Event Severity Levels





Icon and Level	Description
 Critical	Critical-level messages indicate that the software has detected serious problems that will eventually cause a partial or complete failure of a subsystem if not corrected immediately; for example, a power supply failure or rise in temperature must receive immediate attention.
 Error	Error-level messages represent an error condition that does not impact overall system functionality significantly. For example, error-level messages might indicate timeouts on certain operations, failures of certain operations after retries, invalid parameters, or failure to perform a requested operation.

TABLE 4 Event Severity Levels (Continued)

Icon and Level	Description
 Warning	Warning-level messages highlight a current operating condition that should be checked or it might lead to a failure in the future. For example, a power supply failure in a redundant system relays a warning that the system is no longer operating in redundant mode and that the failed power supply needs to be replaced or fixed.
 Info	Information-level messages report the current nonerror status of the system components; for example, the online and offline status of a fabric port.

DISPLAYING FABRIC EVENTS

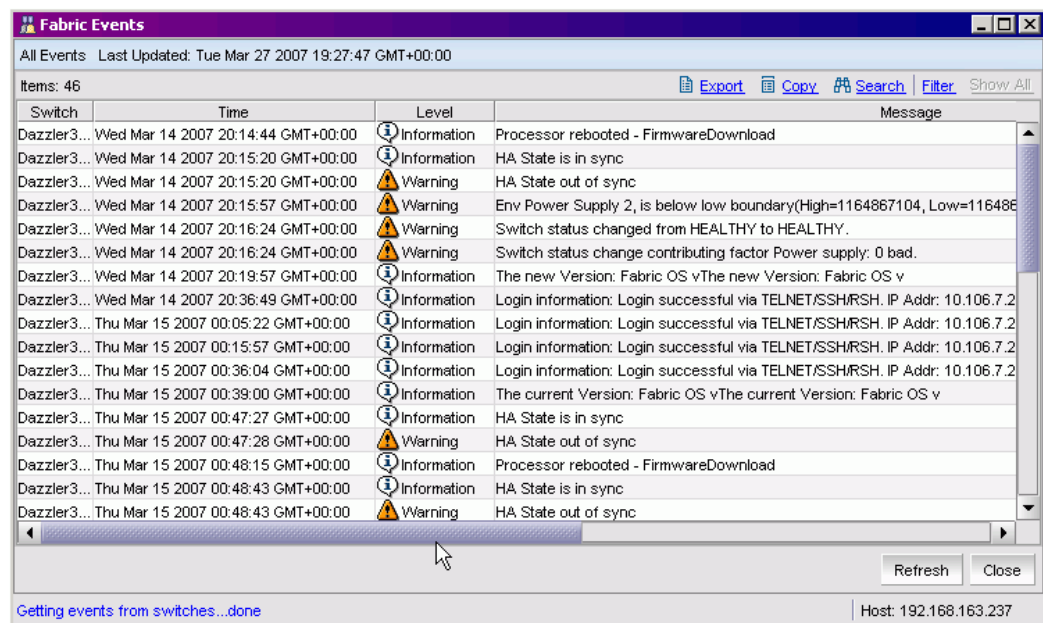
Events are displayed for all switches in the fabric in the Fabric Events window (see [Figure 25](#)). Fabric events are not automatically polled. You must click **Refresh** in the Fabric Events window to poll fabric events.

Fabric Events can be collected only for switches that have the same security level (http or https) as the launch switch. For switches with a different level of security from the launch switch, a message at the top of the window indicates how many switches have no events reported from the last polling. For detailed information on the switch names and reasons for not polling (if available), click **Details**.

To display fabric events

1. Click a fabric in the [Fabric Tree](#).
2. Click **Fabric Events** in the Monitor area under Tasks.

The Fabric Events window displays (see [Figure 25](#)).

**FIGURE 25** Fabric Events window

You can click the column head to sort the events by a particular column, and drag the column divider to resize a column. You can also right-click a column heading to resize one or all columns, sort the information in ascending or descending order, or choose which columns are displayed.

You can also filter events, as described in [“Filtering Fabric and Switch Events”](#) on page 51.

DISPLAYING SWITCH EVENTS

The Switch Events tab displays a running log of events for the selected switch (see [Figure 26](#) on page 50). Switch events are polled and updated every 15 seconds, so there is no refresh-on-demand option for switch events, as there is for the fabric events.

For two-switch configurations, all chassis-related events are displayed in the event list of each logical switch for convenience.

To display switch events

1. Click the switch from the [Fabric Tree](#).
The [Switch View](#) appears.
2. Click the **Switch Events** tab, if necessary.

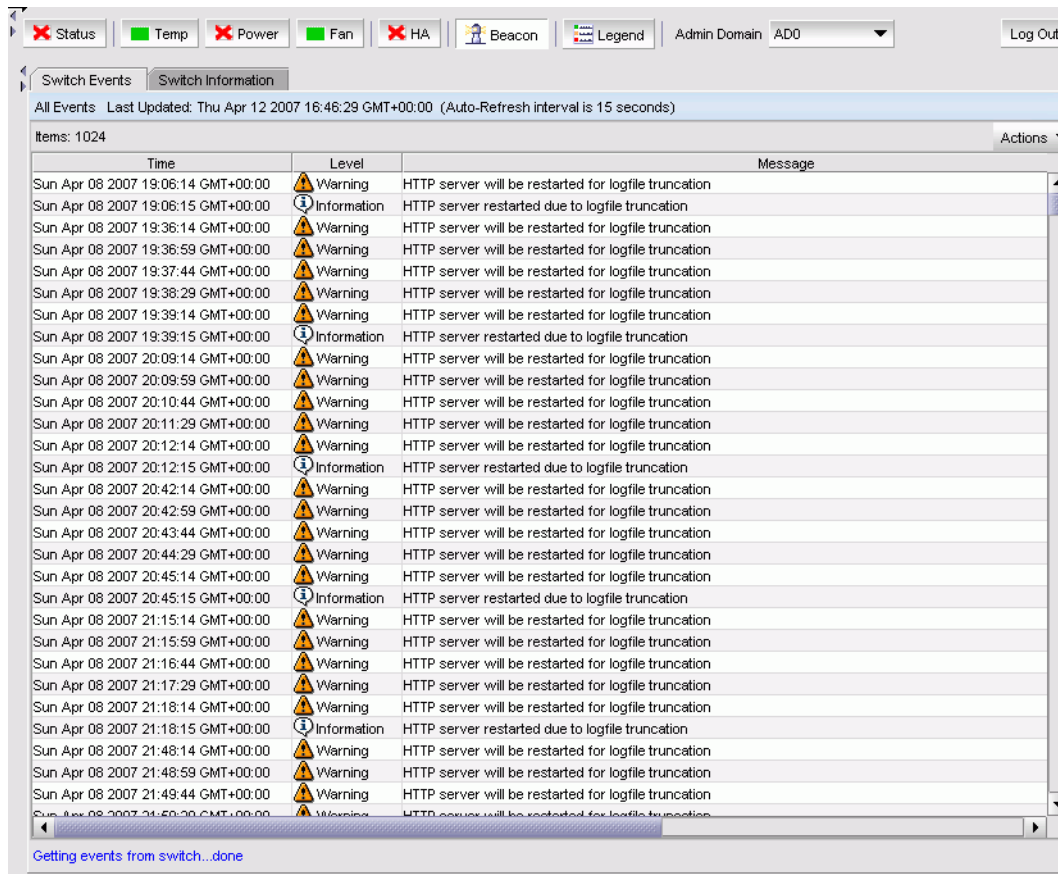


FIGURE 26 Switch Events tab

You can click the column head to sort the events by a particular column, and drag the column divider to resize a column. You can also right-click a column heading to resize one or all columns, sort the information in ascending or descending order, or choose which columns are displayed.

You can also filter events, as described in [“Filtering Fabric and Switch Events,”](#) next.

FILTERING FABRIC AND SWITCH EVENTS

You can filter the fabric and switch events by time, severity, message ID, and service. You can apply either one type of filter at a time or multiple types of filters at the same time. Click the **Filter** button to display the Event Filter dialog box (see [Figure 27](#) on page 51).

When a filter is applied, the filter information appears at the bottom of the filtered information and the **Show All** link is available to allow you to view the information unfiltered.

NOTE

For two-switch configurations, click the **Events** button for a given switch to automatically filter out the switch service events from the other switch. Chassis service is shown in both events lists.

1. Open the Fabric Events window or the Switch Events tab as described in [“Displaying Fabric Events”](#) on page 49 or [“Displaying Switch Events”](#) on page 50.
2. Click **Filter**.

The Event Filter dialog box appears.

FIGURE 27 Event Filter dialog box

3. To filter events within a certain time period:
 - a. Select the **From** check box and enter the start time and date in the fields.
 - b. Select the **To** check box and enter the finish time and date in the fields.
4. To filter events beginning at a certain date and time, select the **From** check box and enter the start time and date.

3 Monitoring events

5. To filter events up until a certain date and time, select the **To** check box and enter the finish time and date.
6. Click **OK**.

The filter is enabled and the window is refreshed to show the filtered information.

To filter events by event severity levels

1. Open the Fabric Events window or the Switch Events tab as described in [“Displaying Fabric Events”](#) on page 49 or [“Displaying Switch Events”](#) on page 50.

2. Click **Filter**.

The Event Filter dialog box appears.

3. Check **Level**.
4. Check the event levels you want to display.
5. Click **OK**.

The filter is enabled and the window is refreshed to show the filtered information.

To filter events by message ID

1. Open the Fabric Events window or the Switch Events tab as described in [“Displaying Fabric Events”](#) on page 49 or [“Displaying Switch Events”](#) on page 50.

2. Click **Filter**.

The Event Filter dialog box displays.

3. Check **Message ID**.
4. Type the message IDs in the associated field.

You can enter multiple message IDs as long as you separate them by commas. You can type either the full message ID (moduleID-messageType) or a partial ID (moduleID only). The message ID filtering is case-sensitive.

5. Click **OK**.

The filter is enabled and the window is refreshed to show the filtered information.

To filter events by service component

1. Open the Fabric Events window or the Switch Events tab as described in [“Displaying Fabric Events”](#) on page 49 or [“Displaying Switch Events”](#) on page 50.

2. Click **Filter**.

The Event Filter dialog box displays.

3. Check **Service**.

The event service drop-down menu is enabled.

4. Select either **Switch** or **Chassis** from the drop-down menu to show only those messages from the logical switch or from the chassis.
5. Click **OK**.

The filter is enabled and the window is refreshed to show the filtered information.

Displaying a fabric summary report

A fabric summary report lists all of the domains in the fabric and the active paths for each domain. A sample fabric summary report is shown in [Figure 28](#) on page 53.

To view a fabric summary report

1. Click **Fabric Summary** in the **Other** section of the **Tasks** menu.

The Fabric Summary window appears.

2. Click the **Print** button to print a topology report.

A **Print** button is located at the top and bottom of the report. Both buttons have the same function.

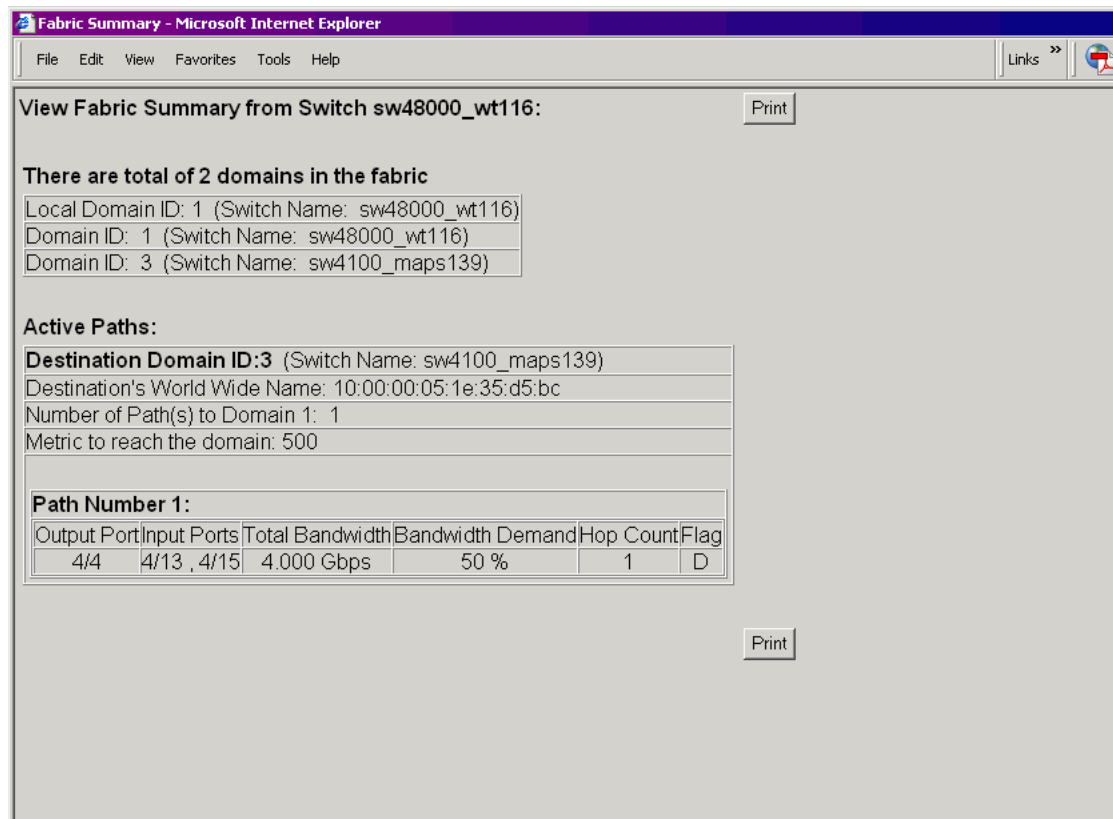


FIGURE 28 Fabric Summary report

Displaying the Name Server entries

Web Tools displays Name Server entries listed in the Simple Name Server database (see [Figure 29](#) on page 54). This includes all Name Server entries for the fabric, not only those related to the local domain. Each row in the table represents a different device.

3 Displaying the Name Server entries

Admin Domain considerations: The Name Server table is filtered based on Admin Domain membership of the fabric devices. The Name Server table shows only devices that are part of the Admin Domain you are currently logged in to. This includes devices that are direct members of the Admin Domain and devices that are attached to ports that are direct members of the Admin Domain. All other fabric devices are filtered out of the Name Server view for the current Admin Domain. See “Admin domain membership” on page 83 for information about direct and indirect members.

To view a list of the switches in the Name Server

1. Click **Name Server** in the **Monitor** section of the **Tasks** menu.

The Name Server window appears.

Domain	Port #	Port ID	Port Type	Device Port WWN	Device Node WWN	Device Name
111	12	6f0c00	N	50:00:51:e3:60:19:01:20	50:00:51:e3:60:19:01:21	IPAddr: 0.0.0.0 Slot/Port: 1/ge4 Logical pn:...
111	106	6f6a00	N	50:00:51:e3:60:19:07:10	50:00:51:e3:60:19:07:11	IPAddr: 0.0.0.0 Slot/Port: 9/ge2 Logical pn:...
3	8	030800	N	10:00:00:00:c9:2e:2b:90	20:00:00:00:c9:2e:2b:90	Emulex LP9002 FV3.90A7 DV5-1.20A7
111	27	6f1be4	NL	21:00:00:20:37:c3:2d:e4	20:00:00:20:37:c3:2d:e4	SEAGATE ST318304FC 0005
111	110	6f6e00	N	50:00:51:e3:60:19:07:30	50:00:51:e3:60:19:07:31	IPAddr: 0.0.0.0 Slot/Port: 9/ge6 Logical pn:...
111	8	6f0800	N	50:00:51:e3:60:19:01:00	50:00:51:e3:60:19:01:01	IPAddr: 200.200.200.80 Slot/Port: 1/ge0 Lo...
111	13	6f0d00	N	50:00:51:e3:60:19:01:28	50:00:51:e3:60:19:01:29	IPAddr: 200.200.200.45 Slot/Port: 1/ge5 Lo...
3	9	0309dc	NL	22:00:00:04:cf:03:4d:4b	20:00:00:04:cf:03:4d:4b	SEAGATE ST318452FC 0002
111	99	6f6300	N	10:00:00:06:2b:0f:73:cd	20:00:00:06:2b:0f:73:cd	LSI7404XP-LC BR A,1 03-01081-02D FW:...
111	9	6f0900	N	50:00:51:e3:60:19:01:08	50:00:51:e3:60:19:01:09	IPAddr: 0.0.0.0 Slot/Port: 1/ge1 Logical pn: 9
111	107	6f6b00	N	50:00:51:e3:60:19:07:18	50:00:51:e3:60:19:07:19	IPAddr: 0.0.0.0 Slot/Port: 9/ge3 Logical pn:...
111	111	6f6f00	N	50:00:51:e3:60:19:07:38	50:00:51:e3:60:19:07:39	IPAddr: 0.0.0.0 Slot/Port: 9/ge7 Logical pn:...
3	9	0309e2	NL	22:00:00:04:cf:03:4d:15	20:00:00:04:cf:03:4d:15	SEAGATE ST318452FC 0002
111	104	6f6800	N	50:00:51:e3:60:19:07:00	50:00:51:e3:60:19:07:01	IPAddr: 0.0.0.0 Slot/Port: 9/ge0 Logical pn:...
111	108	6f6c00	N	50:00:51:e3:60:19:07:20	50:00:51:e3:60:19:07:21	IPAddr: 0.0.0.0 Slot/Port: 9/ge4 Logical pn:...
3	9	0309e0	NL	22:00:00:04:cf:03:49:bc	20:00:00:04:cf:03:49:bc	SEAGATE ST318452FC 0002
111	10	6f0a00	N	50:00:51:e3:60:19:01:10	50:00:51:e3:60:19:01:11	IPAddr: 200.200.200.91 Slot/Port: 1/ge2 Lo...
111	27	6f1bef	NL	21:00:00:20:37:c3:2d:56	20:00:00:20:37:c3:2d:56	
111	105	6f6900	N	50:00:51:e3:60:19:07:08	50:00:51:e3:60:19:07:09	IPAddr: 0.0.0.0 Slot/Port: 9/ge1 Logical pn:...
111	11	6f0b00	N	50:00:51:e3:60:19:01:18	50:00:51:e3:60:19:01:19	IPAddr: 0.0.0.0 Slot/Port: 1/ge3 Logical pn:...
3	9	0309e4	NL	22:00:00:04:cf:03:49:d1	20:00:00:04:cf:03:49:d1	SEAGATE ST318452FC 0002

FIGURE 29 Name Server window

You can click the column head to sort the events by a particular column, and drag the column divider to resize a column. You can also right-click a column heading to resize one or all columns, sort the information in ascending or descending order, or choose which columns are displayed.

2. To set an autorefresh rate, select the **Auto Refresh** check box in the Name Server window, and type an auto-refresh interval (in seconds).

The minimum (and default) interval is 15 seconds.

The Name Server entries will refresh at the rate you set.

To print the Name Server entries

1. Click **Name Server** in the Monitor section of the Tasks menu.

The Name Server window appears.

2. Click **Print**.

3. On the Page Setup dialog box, make the changes specific to your printing preferences and click **OK**.

The Print dialog box appears.

4. Select a printer and click **OK** in the Print dialog box.

To display detailed Name Server information for a particular device

1. Click **Name Server** in the **Monitor** section of the **Tasks** menu.

The Name Server window appears.

2. Click a device from the Domain column.
3. Click **Detail View**.

The Name Server Information dialog box displays information specific to that device.

To display the zone members of a particular device

1. Click **Name Server** in the **Monitor** section of the **Tasks** menu.

The Name Server window appears.

2. Click a device from the Domain column.
3. Click **Accessible Devices**.

The Zone Accessible Devices window displays accessible zone member information specific to that device.

Physically locating a switch using beaconing

Use the **Beacon** button to physically locate a switch in a fabric. The beaconing function helps to physically locate a switch by sending a signal to the specified switch, resulting in an LED light pattern that cycles through all ports for each switch (from left to right).

NOTE

Switch beaconing is enabled when the switch is owned by the current Admin Domain you are logged in to or if the account you are logged in with is associated with an administrator role; otherwise, switch beaconing is disabled.

To enable beaconing

1. Select a switch from the [Fabric Tree](#).

The selected switch appears in the [Switch View](#).

2. Click the **Beacon** button on the [Switch View](#).

The LED lights on the actual switch (selected in the GUI) light up on the physical switch in a pattern running back and forth across the switch itself. The beaconing is not shown in the GUI.

3. Look at the physical switches in your installation location to identify the switch.

3 Physically locating a switch using beaconing

Maintaining Configurations and Firmware

This chapter contains the following information:

- [“Maintaining configurations,”](#) next
- [“Performing a firmware download”](#) on page 60

Maintaining configurations

It is important to maintain consistent configuration settings on all switches in the same fabric, because inconsistent parameters (such as inconsistent PID formats) can cause fabric segmentation. As part of standard configuration maintenance procedures, it is recommended that you back up configuration data for every switch on a host computer server for emergency reference.

This section contains procedures for basic switch configuration maintenance. Use the **Configure** tab and **Upload/Download** subtab of the Switch Administration window to perform these tasks. See [Figure 30](#) for details.

ATTENTION

It is recommended that you are in AD255 or ADO, when no other user-defined Admin Domains exist, to perform a config upload/download to gather *all* the configuration files for the fabric, including Admin Domains and iSCSI Target Gateway information.

4 Maintaining configurations

SwitchName: Dazzler3850 DomainID: 1 VVNN: 10:00:00:05:1e:34:00:70 Mon Apr 02 2007 18:43:59 GMT+00:00

Configure Routing Extended Fabric AAA Service Trace FICON CUP ACL Distribution IPFilter

Switch Network Firmware Download License User Trunking SNMP

Function

☒ Config Upload to Host ☐ Config Download to Switch

Host IP File Name

User Name Password

Select Protocol : ☒ FTP ☐ SCP

Upload/Download Progress:

Fabric Virtual Channel Arbitrated Loop System Upload/Download

Apply Close Refresh

[Switch Administration opened]: Mon Apr 02 2007 18:43:07 GMT+00:00

Configure Switch Parameters Mode: Advanced 192.168.163.237 AD0 User: admin Role: admin

FIGURE 30 Configure tab, Upload/Download subtab

BACKING UP A CONFIGURATION FILE

Keep a backup copy of the configuration file in case the configuration is lost or unintentional changes are made. You should keep individual backup files for all switches in the fabric. You should avoid copying configurations from one switch to another.

When you back up a configuration file for a Brocade 24000 configured with two logical switches, it is on a logical-switch basis. This means that you must back up a separate configuration file for each logical switch.

Admin Domain considerations: When you log in to the switch as a physical fabric administrator and back up a configuration, all local switch configuration parameters are saved, as well as all Admin Domain membership information and Admin Domain zone databases.

When the configuration is backed up one of the following scenarios are possible:

- If the current Admin Domain does not own the switch and you are logged in with any role that allows config upload/download, the following will be saved in the config file:
 - Local zone configuration
 - iSCSI configuration (if any)
 - No other configuration information
- If the current Admin Domain *owns the switch* and you are logged in with any role that allows config upload/download, the following will be saved in the configuration file:
 - Local zone configuration

- iSCSI config (if any)
- All other config information except Admin Domain configuration information
- If you invoke it from AD255 and you are logged in with any role that allows config upload/download, the following will be saved in the configuration file:
 - Configuration information for zones in all Admin Domains
 - iSCSI configuration (if any)
 - All other configuration information, including zoning from all Admin Domains

The filtering depends on the Admin Domain switch ownership, with additional access if you are in AD255. Access to the command itself is limited by Role-based access (RBAC), and not by whether the current user is a Physical Fabric Administrator or an admin user with enumerated access to the relevant domains.

To back up a configuration file

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **Configure** tab.
3. Click the **Upload/Download** subtab (see [Figure 30](#)).
4. Click the **Config Upload to Host** radio button.
5. Type the host IP, user name, file name, and password.
You can enter the IP address in either IPv4 or IPv6 format.
6. Type the configuration file with a fully qualified path.
7. Select a protocol to use to transfer the file.
8. Click **Apply**.

You can monitor the progress by looking at the Upload/Download progress bar.

RESTORING A CONFIGURATION

Restoring a configuration involves overwriting the configuration on the switch by downloading a previously saved backup configuration file. Perform this procedure during a planned down time.

Make sure that the configuration file you are downloading is compatible with your switch model, because configuration files from other model switches might cause your switch to fail.

To download a configuration to the switch

1. Open the Switch Administration window as described on [page 31](#).
2. Disable the switch, as described in [“Enabling and disabling a switch”](#) on page 37.
You can download configurations only to a disabled (offline) switch. You will only be able to disable the switch if you the Admin Domain you are logged into owns the switch.
3. Click the **Configure** tab.
4. Click the **Upload/Download** subtab (see [Figure 30](#) on page 58).
5. Click the **Config Download to Switch** radio button.
6. Type the host IP, user name, file name, and password.
You can enter the IP address in either IPv4 or IPv6 format.

4 Performing a firmware download

7. Type the configuration file with a fully qualified path.
8. Select a protocol to use to transfer the file.
9. Click **Apply**.

You can monitor the progress by looking at the Upload/Download progress bar.

10. Enable the switch, as described in [“Enabling and disabling a switch”](#) on page 37.

Performing a firmware download

During a firmware download, the switch reboots and the browser temporarily loses connection with the switch. When the connection is restored, the version of the software running in the browser is different from the new software version that has been installed and activated on the switch. You will need to close all of the Web Tools windows and re-log in to avoid a firmware version mismatch. Note that for chassis-based switches, you might get popup messages that imply the loss of connection is temporary and will soon be resolved. You still need to close all windows and re-log in.

When you request a firmware download, the system first checks the file size that is to be downloaded. If the compact flash does not have enough space, Web Tools displays a message and the download does not occur. If this happens, contact your switch support supplier.

NOTE

You can perform a firmware download only when the current Admin Domain owns the switch.

To download a new version of the firmware

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **Firmware Download** tab.

The screenshot shows the 'Firmware Download' tab in the Switch Administration window. At the top, there is a header bar with a 'Show Advanced Mode' button. Below the header, the following information is displayed: SwitchName: Stealth200E, DomainID: 2, VVWN: 10:00:00:05:1e:01:23:e0, and Tue Feb 06 2007 11:45:59 GMT+00:00. The main content area has several tabs: Switch, Network, Firmware Download (selected), License, User, and Trunking. Under the 'Firmware Download' tab, there are two sections. The first section, 'Current Firmware Information', shows 'Primary partition: 5.3.0_main_bld10' and 'Secondary partition: 5.3.0_main_bld10'. The second section, 'Download New Firmware', contains a sub-header 'Provide Host Details, Transfer Protocol and Path for Firmware Download' and several input fields: 'Host Name or IP', 'User Name', 'Password', 'Protocol Type' (set to 'File Transfer Protocol (FTP)'), and 'Specify Firmware Path'. At the bottom right of the form are three buttons: 'Download', 'Close', and 'Refresh'.

FIGURE 31 Firmware Download tab

3. Type the host name or IP address, user name, password, and fully qualified path to the file *release.plist*.

You can enter the IP address in either IPv4 or IPv6 format.

The path name should follow the structure below:

```
//<directory>/<fos_version_directory>/release.plist
```

where the *<directory>* is the path up to the entry point of *<fos_version_directory>* and *<fos_version_directory>* is where the unzipped version of Fabric OS has been put. For example:

```
//directory_1/my_directory/v5.2.0/release.plist
```

4. Select the protocol type in the Protocol Type field.
If you choose “Secure Copy Protocol (SCP),” you cannot specify “anonymous” in the User field.
5. Click **Apply**.
The firmware download begins. You can monitor the firmware download status on the Firmware Download progress bar.
About halfway through the download process, connection to the switch is lost and Web Tools invalidates the current session. (Web Tools invalidates all windows if upfront login is enabled.)
6. Close all Web Tools windows and log in again.
If the firmware download is in progress when you log in, you can continue to monitor its progress.

SAS and SA firmware download for SW7600 and FC4-18 blade platforms

If you are downloading SAS and DMM firmware directly to the blade, you have more options on the Firmware Download tab, as shown in [Figure 32](#). Also, for Brocade 7600, a collapsible area appears on the Firmware Download tab to show application firmware information

In addition to specifying the information described in the steps on [page 60](#), you can choose:

- Whether to download the firmware or the firmware key.
- The type of firmware you want to be downloaded.
- The firmware path. Web Tools displays up to 15 path entries in the Specify Firmware Path field.
- To download the firmware even if it is not compatible (skip version check).
- To enable removal of application firmware (erase SA).

4 Performing a firmware download

- The blade to be upgraded (by slot).

The screenshot shows the 'Firmware Download' tab of a switch management interface. At the top, there's a header with 'SwitchName: wtQA_satur91', 'DomainID: 91', 'WWN: 10:00:00:60:69:e4:00:36', and 'Tue May 29 2007 19:41:16 IST'. Below this is a navigation bar with tabs: 'Switch', 'Network', 'Firmware Download' (selected), 'License', 'User', 'Blade', and 'Trunking'. A 'Show Advanced Mode' button is in the top right.

The main content area is divided into two sections. The first, 'Current Firmware Information', shows 'Local CP (Active)' and 'Remote CP (Standby)' with their respective FOS Primary and Secondary Partitions, all listed as '5.3.0_rel_bld45'. The second section, 'Download New Firmware', contains two steps:

- Step 1: Select Type of Firmware to be Downloaded**
A dropdown menu for 'Select Firmware Type' is set to 'sas'.
- Step 2: Provide Host Details *, Transfer Protocol and Path for Firmware Download**
A red note states: '*Password is optional, if user name is "anonymous"'.
Fields include:
 - Host Name or IP: 10.32.2.25
 - User Name: jewell
 - Password: masked with dots
 - Protocol Type: File Transfer Protocol (FTP) (dropdown)
 - Specify Firmware Path: /pubs/sre/SQA/fos/v5.3.0 (dropdown)

Below Step 2 are checkboxes for 'Skip Version Check' and 'Erase SA'. A 'Blades to be upgraded' section has a 'Slot(s):' field with the value '3'. At the bottom right of the form are 'Download', 'Close', and 'Refresh' buttons.

A status bar at the bottom shows 'Firmware download' on the left and 'Mode: Basic | 10.33.13.91 | AD0 | User: admin | Role: admin' on the right. A log message at the bottom left reads '[Switch Administration opened]: Tue May 29 2007 19:35:52 IST'.

FIGURE 32 Firmware Download tab for bladed switches

Managing Your Ports

This chapter describes how to manage FC and gigabit Ethernet (GbE) ports. See [“Viewing and configuring EX_Ports”](#) on page 140 for information on how to view and configure EX_Ports.

In this chapter

This chapter contains the following sections:

- [Viewing and managing ports using Web Tools](#) 63
- [Configuring ports](#) 67
- [Assigning a name to a port](#) 70
- [Enabling and disabling a port](#) 71
- [Persistent enabling and disabling ports](#) 71
- [Enabling and disabling NPIV ports](#) 72
- [Activating ports](#) 73
- [Swapping port index](#) 75

Viewing and managing ports using Web Tools

You can view and manage ports through the Port Administration window, shown in [Figure 33](#) on page 64. You access the Port Administration window through the Switch View, by clicking an accessible port. See [“Switch View”](#) on page 21 for information about accessible ports.

The Port Administration window is refreshed automatically every two minutes and is refreshed immediately when you make any port changes through Web Tools.

To manage ports, you must be logged in with the role of switchadmin, admin, basicswitchadmin, operator, or fabricadmin. If you are logged in with a user, securityadmin, or zoneadmin role, you can only view the port information.

To open the Port Administration window

- 1. Click an accessible port in the [Switch View](#) to open the Port Administration window.
The window opens in basic mode (see [Figure 33](#)).

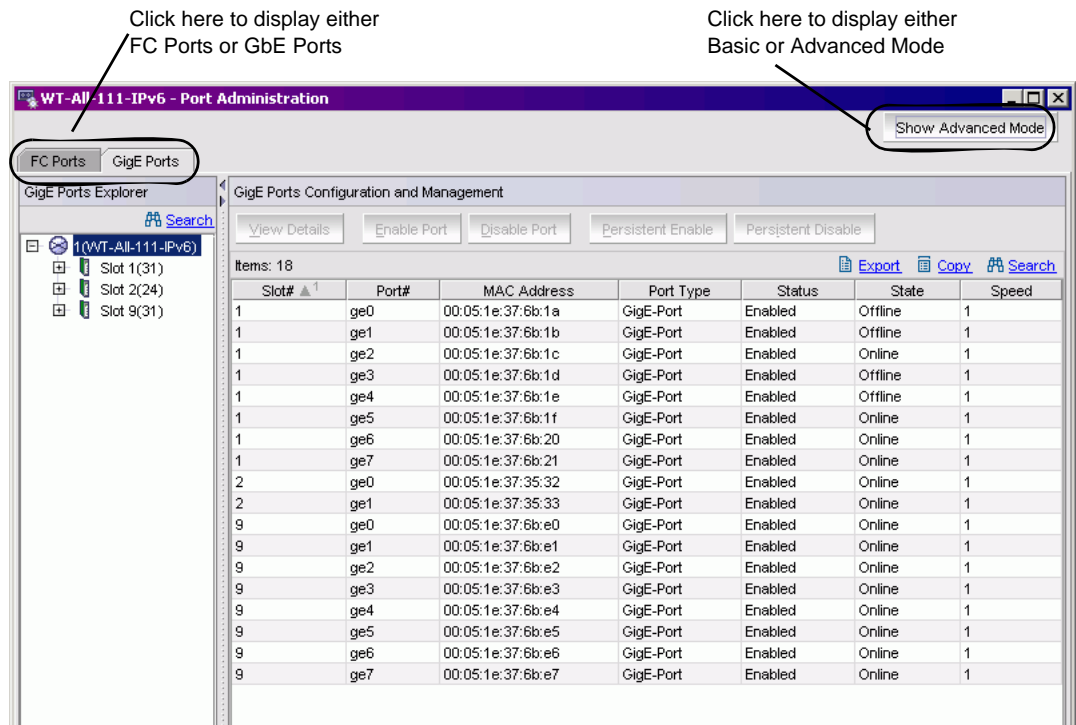


FIGURE 33 Port Administration window, GigE Ports, Basic mode

The Port Administration window displays information about the ports on the switch. Click the **Show Advanced Mode** button in the upper-right corner of the window to see more port management options (see [Figure 33](#)).

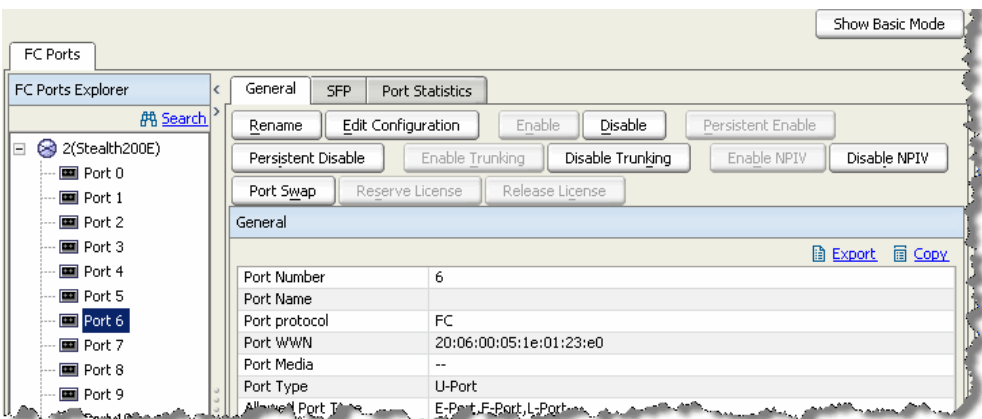


FIGURE 34 Port Administration window, FC Ports General Advanced mode detail

Admin Domain considerations: In fabrics where there are user-defined Admin Domains, the Port Administration window is filtered to show only ports that are *direct* or *indirect* members of the currently selected Admin Domain.

- Direct members are ports that have been directly added to the Admin Domain as members.
- Indirect members are:
 - non-owned ports on a member switch
 - non-owned ports to which member devices are attached
- All active ports, as well as any inactive EX_ports are shown.

PORT ADMINISTRATION WINDOW COMPONENTS

The Port Administration window (shown in [Figure 33](#)) has the following components:

- Two tabs on the top left: **FC Ports** and **GigE Ports**. If the switch does not have GbE ports, the **GigE Ports** tab does not appear.
 - To display all of the FC ports on the switch (physical FC ports and logical FCIP ports), click the **FC Ports** tab.
 - To display all of the GbE ports, click the **GigE Ports** tab.
On the FR4-18i blade, each GbE port can have up to eight logical FCIP ports. These FCIP ports are displayed in the **FC Ports** subtab. FC4-16IP GigE ports are also displayed.
- A Ports Explorer tree on the left side. Items in the tree are displayed as follows:
 - Switches—Switch ID, with switch name in parentheses; for example, 3(MapsSW_202)
 - Blades—Slot number of the blade, with blade ID in parentheses; for example, Slot 7(24)
 - Ports—Port number; for example, Port 2
- Button area. The button area contains buttons for all the tasks you can perform on the selected port. If you select more than one port, buttons are available for only the tasks that you can perform on all of the selected ports. Buttons are grayed (unavailable) if they are not applicable to the selected ports.
- Port information appears in either a table of ports or information about a specific port, depending on your selection:
 - If you select a slot or switch, the system displays a table of all the ports for the slot or switch (see [Figure 35](#) on page 67).
 - If you select a port, the system displays detailed information about the port (see [Figure 34](#)).
You can choose to view either Basic mode or Advanced mode, and to view the subtabs which contain additional information about the port. The available subtabs depend on the type of port selected.
- When viewing detailed information about a port, Basic mode provides these subtabs:
 - General—All ports
 - Rename
 - Edit Configuration
 - Enable/Disable (port)
 - Persistent Enable/Persistent Disable (port)
 - SFP—Physical ports only (FC and GbE)
 - Basic information about the port equipment

- Port Statistics—All ports
 - Basic port information and statistics

Note that on the **Port Statistics** subtab, you can view either absolute values or deltas for port statistics. Viewing the deltas is useful if you want to view current port trends. To reset the counters on the port statistics, click the **Clear Counters** button.

FCIP statistics for a GbE port are the accumulated statistics of all the FCIP tunnels for that GbE port.
- IP Interfaces—GbE ports only
- IP Routes—GbE ports only
- When viewing detailed information about a port, the Advanced mode provides these additional subtabs:
 - General—All ports
 - Enable/Disable Trunking
 - Enable/Disable NPIV
 - Port Swap
 - Reserve License
 - Release License
 - SFP—Physical ports only (FC and GbE)
 - Advanced information about the port equipment
 - Port Statistics
 - Advanced port statistics
 - FCIP Tunnels—GbE ports and logical FCIP ports only (not available for the FR4-16IP)

IDENTIFYING CONTROLLABLE PORTS

All ports have a “Controllable” attribute visible from the Advanced Mode, which represents a combination of the RBAC and Admin Domain permissions. [Figure 35](#) shows the Controllable attribute.

The Controllable attribute is **No** in the following situations:

- If your account has read-only permission, all accessible ports display in read-only mode, regardless of the Admin Domain context. All configuration functionality is disabled.
- Non-owned E_Ports and indirect member ports on non-owned switches are accessible in read-only mode and are not controllable, regardless of RBAC permissions.

The Controllable attribute is **Yes** for ports that are directly owned by the current Admin Domain and for all ports on switches that are owned by the current Admin Domain, if your role gives you Modify permission for ports. If a port is controllable, all configuration functionality is enabled.

Ports on a non-owned switch that are not E_Ports and are neither direct nor indirect members of the current Admin Domain are inaccessible and are not displayed in the Port Administration window.

FC Ports Explorer

Search

Item Selected: 1

Port.#	Port Name	Port Status	Health	Port Type	Speed (Gb/s)	Controllable	Licensed	Trunking Enabled	NPIV Enabled	Additional Po...
0		Online	Healthy	E-Port	N2	Yes	Yes	true	true	(Segmented...)
1		No_Module	Offline	U-Port	N4	Yes	Yes	true	true	
2	Name 2	Online	Healthy	F-Port	N2	Yes	Yes	true	true	
3		No_Module	Offline	U-Port	N4	Yes	Yes	true	true	
4		No_Module	Offline	U-Port	N4	Yes	Yes	true	true	
5		No_Module	Offline	U-Port	N4	Yes	Yes	true	true	
6		No_Module	Offline	U-Port	N4	Yes	Yes	true	true	
7		No_Light	Offline	U-Port	2	Yes	Yes	false	false	
8	Name 8	Online	Healthy	F-Port	N2	Yes	Yes	true	true	
9	Name 9	No_Module	Offline	U-Port	N4	Yes	Yes	true	true	
10		No_Module	Offline	U-Port	N4	Yes	Yes	true	true	
11		No_Module	Offline	U-Port	N4	Yes	Yes	true	true	
12		Disabled	Offline	U-Port	N4	Yes	No	true	true	None
13		Disabled	Offline	U-Port	N4	Yes	No	true	true	None
14		Disabled	Offline	U-Port	N4	Yes	No	true	true	None
15		Disabled	Offline	U-Port	N4	Yes	No	true	true	None

Mode: Advanced Host: 192.168.163.238 AD: AD0 User: admin Role: admin

Figure 35 Port Administration window, Table view

Configuring ports

Web Tools provides wizards to assist you in configuring ports. This section describes how you can configure FC ports, logical FCIP ports, GbE ports, and NPIV ports.

CONFIGURING FC PORTS

With the FC Port Configuration wizard, you can configure allowed port types, port speed, and long distance mode for physical ports.

The following procedure describes how to open the FC Port Configuration wizard. The wizard is self-explanatory, so the explicit steps are not documented here.

To configure FC ports

1. Click a port in the Switch View to open the Port Administration window (see [Figure 33](#) on page 64).
2. Click the **FC Ports** tab.

5 Configuring ports

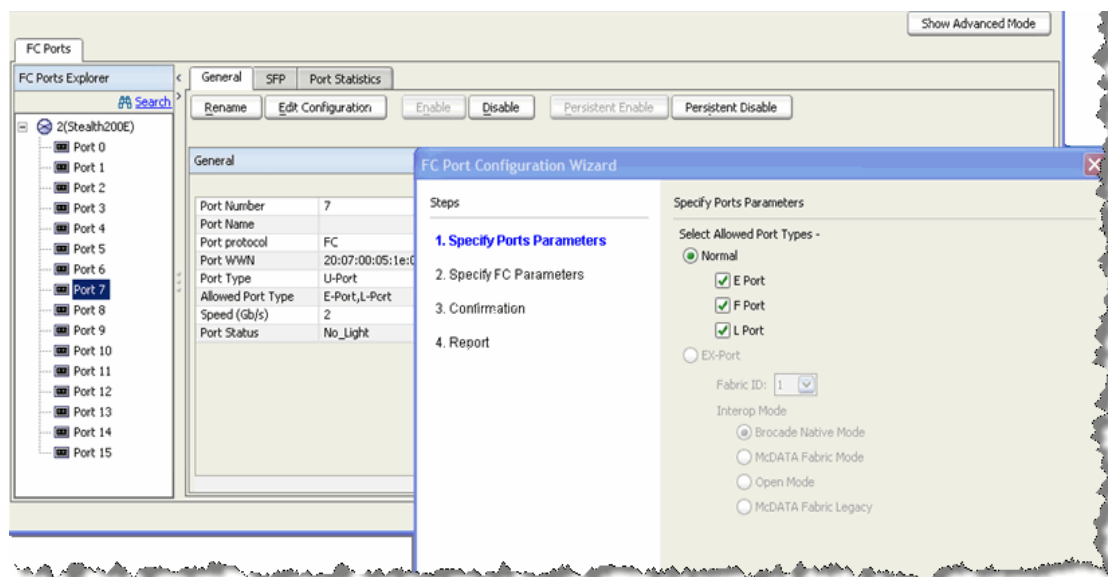


FIGURE 36 FC Port Configuration Wizard, FC ports

3. From the tree on the left, select the port you want to configure.
4. Click the **General** subtab.
5. Click the **Edit Configuration** button.

The FC Port Configuration wizard opens. The fields are populated with the current configuration values.

6. Follow the steps in the wizard.

If you configure a disabled port as an EX_Port, the wizard displays the **Enable Port after configuration** check box. If you select the check box, the disabled port is automatically enabled after configuration; otherwise, the port remains in the same state after configuration.

Allowed Port Types

For FC ports, the Port Administration window displays the following values relating to port type:

Port Type This is the actual or current port type. If the port is offline, this value is the allowed types (or U_Port, if no type constraint has been specified). If the port is online, this value is the type the port has actually negotiated to.

Allowed Port Type The allowed or configured port type.

The allowed port types indicate any constraints on what types the port can negotiate to when it comes up. For normal (that is, non-EX_Port) ports, the following are the allowed port types:

L_Port The port can be used to connect a loop device.

F_Port The port can be used to connect a non-loop device.

E_Port The port can be used to connect to another switch.

U_Port For a physical FC port: the port can be any one of E_Port, F_Port, or L_Port. For a logical FC port: the port can be either VE_Port or VEX_Port.

When the wizard prompts you to select allowed port types, if all of these boxes are selected, there are no constraints on port type. The port will negotiate to its preferred type when the switch comes up, depending on what type of device or switch it is connected to.

Clearing a check box guarantees that the port will *not* attempt to function as a port of the unchecked type. At least one type must remain selected. L-Port and F-Port cannot both be cleared.

NOTE

To configure a port as an EX_Port, the switch must be capable of supporting FCR/FCIP features. The EX_Port option is disabled in the wizard if the switch does not meet these requirements.

Long distance mode

Port long distance configuration can be performed here and in the Switch Admin Extended Fabric tab. For information about long distance mode settings, see [Chapter 13, “Administering Extended Fabrics”](#).

FC Fastwrite

FC Fastwrite reduces the number of round-trip times required to write data.

For Brocade 48000 and 7500 switches, you can enable FC Fastwrite. When FC Fastwrite is enabled, all GigE port and FCIP features are disabled.

CONFIGURING FCIP PORTS

With the FC Port Configuration wizard, you can configure the port type for logical FCIP ports.

Configure the port to be a VE_Port if you want to merge with the remote fabric with which you are communicating. Configure the port to be a VEX_Port if you want to communicate with a remote fabric without merging with it.

Admin Domain considerations: You can configure FCIP ports only when the current Admin Domain owns the switch.

The following procedure describes how to open the FC Port Configuration wizard. The wizard is self-explanatory, so the explicit steps are not documented here.

To configure FCIP ports

1. Click a port in the Switch View to open the Port Administration window.
2. Click the **FC Ports** tab.
3. From the tree on the left, select the logical port you want to configure.
4. Click the **General** subtab.
5. Click the **Edit Configuration** button.

The FC Port Configuration wizard opens. The fields are populated with the current configuration values.

6. Follow the steps in the wizard.

For VEX_Ports, you will need to specify the Fabric ID. You can choose any unique fabric ID as long as it is consistent for all VEX_Ports that connect to the same edge fabric.

If you configure a disabled port as a VEX_Port, the wizard provides the **Enable Port after configuration** check box. If you select this check box, the disabled port is automatically enabled after configuration. If you leave this check box cleared, the port remains in the same state after configuration.

CONFIGURING GBE PORTS

With the GigE Port Configuration wizard, you can configure IP interfaces, and IP routes.

For setting up iSCSI Target Gateway, please see [Chapter 14, “Administering the iSCSI Target Gateway”](#).

Admin Domain considerations: You can configure GbE ports only when the current Admin Domain owns the switch.

The following procedure describes how to open the GigE Port Configuration wizard. The wizard is self-explanatory, so the explicit steps are not documented here.

To configure GbE ports

1. Click a port in the Switch View to open the Port Administration window (see [Figure 33](#) on page 64).
2. Click the **GigE Ports** tab.
3. Select the port you want to configure in the tree on the left side of the window.
4. Click **Edit Configuration** in the task bar.

The GigE Port Configuration wizard opens. The wizard fields are populated with the current configuration values.

5. Follow the steps in the wizard.

Assigning a name to a port

Port names are optional. You can assign a name to an FC or FCIP port to make port grouping easier. You can rename FC and FCIP ports too. You cannot rename GbE ports. The Port Name column in the **Ports** tab displays the port name, if one exists.

Port names can be from 1 through 32 alphanumeric characters, unless Ficon Management Server (FMS) mode is enabled; if FMS mode is enabled, port names should be limited from 1 through 24 alphanumeric characters. The comma (,), semicolon (;), and “at” symbol (@) are not allowed.

Although it is not required that port names be unique, it is recommended.

To rename a port

1. Click a port in the Switch View to open the Port Administration window.
2. Click the **FC Ports** tab.
3. From the tree on the left, click the switch or slot that contains the port you want to rename.
4. From the table, select the port you want to rename.
5. Click the **Rename** button.

6. Type a name for the port and click **Rename**.

To delete the existing port name, leave the field blank and click **Rename**.

Enabling and disabling a port

On FR4-18i and FC4-16IP port blades, all ports are disabled by default. You can disable and reenable them as needed.

If FC Routing is disabled, all EX_Ports are automatically disabled and you cannot enable them until FC Routing is enabled.

If a port is not licensed you cannot enable it until you install the appropriate license, such as a **Ports on Demand** or **N-Port ID Virtualization** license (see [“Activating ports”](#) on page 73 for more information). The **Licensed** field located in the **General** tab in the **Port Administration** window indicates whether a port is licensed.

If you disable a *principal* ISL port (an ISL port that has been designated by the fabric to be a part of the path to communicate with the principal switch), the fabric reconfigures.

If you disable a port that was connected to a device, that device is no longer accessible from the fabric. For more information, see the *Fabric OS Administrator's Guide*.

To enable or disable ports

1. Click a port in the Switch View to open the Port Administration window.
2. Click the **FC Ports** or **GigE Ports** tab.
3. From the tree on the left, click the switch or slot that contains the port you want to enable or disable.
4. From the table, select one or more ports.

Use Shift-click and Ctrl-click to select multiple ports. You can select multiple ports from the table. You cannot select multiple ports from the tree.

5. Click the **Enable** or **Disable** button.

If the button is gray (unavailable), the port is already in the enabled or disabled state. For example, if the **Enable** button is unavailable, the port is already enabled.

If you select multiple ports in both enabled and disabled states, both buttons are active. When you click either button, the action is applied to all selected ports.

6. Click **Yes** in the confirmation window.

Persistent enabling and disabling ports

Use the following procedure to enable or disable an FC port so that it remains enabled or disabled across switch reboots.

NOTE

Ports cannot be persistently enabled or disabled when FMS is enabled.

To enable or disable a port over reboots

1. Click a port in the Switch View to open the Port Administration window.
2. Click the **FC Ports** or **GigE Ports** tab.
3. From the tree on the left, click the switch or slot that contains the port.
4. From the table, select one or more ports.

Use Shift-click and Ctrl-click to select multiple ports. You can select multiple ports from the table. You cannot select multiple ports from the tree.

5. Click the **Persistent Enable** or **Persistent Disable** button.

If the button is gray (unavailable), the port is already in that state. For example, if the **Persistent Enable** button is unavailable, the port or ports are already persistently enabled over reboots.

If you select multiple ports in both enabled and disabled states, both buttons are active. When you click either button, the action is applied to all selected ports.

6. Click **Yes** in the confirmation window.

Enabling and disabling NPIV ports

N-Port ID Virtualization (NPIV) enables a single Fibre Channel protocol port to appear as multiple, distinct ports, providing separate port identification within the fabric for each operating system image behind the port (as if each operating system image has its own unique physical port). NPIV assigns a different virtual port ID to each Fibre Channel protocol device. NPIV enables you to allocate virtual addresses without impacting your existing hardware implementation. The virtual port has the same properties as an N_Port, and is therefore capable of registering with all services of the fabric.

The NPIV license must be installed on a switch before NPIV functionality can be enabled on any port.

NOTE

NPIV enable/disable is not supported on EX_Ports.

To configure NPIV ports, see the *Fabric OS Administrators Guide*. Web Tools allows you only to enable or disable the NPIV functionality on a port.

To enable NPIV ports

1. Click a port in the Switch View to open the Port Administration window.
2. Click the **FC Ports** tab.
3. From the tree on the left, select the logical port you want to enable.
4. Click the **Enable NPIV** button.

The button is unavailable if NPIV is already enabled on the port.

To disable NPIV ports

1. Click a port in the Switch View to open the Port Administration window.
2. Click the **FC Ports** tab.

3. From the tree on the left, select the logical port you want to disable.
4. Click the **Disable NPIV** button.

The button is unavailable if NPIV is already disabled on the port.

Activating ports

Brocade switches come with a preset number of ports enabled. Additional ports can be enabled using the Ports on Demand licenses and the Dynamic Ports on Demand feature (for supported switches only).

Ports on Demand is ready to be unlocked in the switch firmware. Its license might be part of the licensed Paper Pack supplied with switch software, or you can purchase the license separately from your switch vendor, who will provide you with a key to unlock it. You can install up to two Ports on Demand licenses on each switch.

[Table 5](#) shows the ports that are enabled by default and the ports that can be enabled after you install the first and second Ports on Demand licenses for each switch type, and the ports that can be enabled with the Dynamic PODs feature.

TABLE 5 Ports Enabled with POD Licenses and DPOD Feature

Switch Name	Enabled by Default	Enabled with Ports on Demand License(s)	Enabled with the Dynamic Ports on Demand Feature
Brocade 200E	0-7	8-11 12-15	Not supported
Brocade 5000 Brocade 4100	0-15	16-23 24-31	Not supported
Brocade 4016	0-7, 10-13	8, 9, 14, 15	Any available ports
Brocade 4018	2-11	12-17	Any available ports
Brocade 4020	0-7, 15, 16	8, 9, 17-19 10-14	Any available ports
Brocade 4024	1-8, 17-20	9-12, 21, 22 0, 13-16, 23	Any available ports
Brocade 4900	0-31	32-47 48-63	Not supported

For the Brocade 4016, 4018, 4020, and 4024 switches *only*, you can use the Dynamic Ports on Demand (DPOD) feature, which allows you to choose which ports to enable (instead of predefined sets of ports) after the POD license(s) is installed. Web Tools allows you only to enable or disable the DPOD functionality on a port. To configure DPOD, see the *Fabric OS Administrator's Guide*.

In the Port Administration window, the *Licensed* attribute indicates whether a port is licensed (yes), whether it can be license (possible) because there are free licenses available (only applicable with the Dynamic POD feature), or whether it is not licensed and cannot be licensed because there is no available license.

After the license keys are installed, you must enable the ports. You can do so without disrupting switch operation, as described in [“Enabling and disabling a port”](#) on page 71. Alternatively, you can disable and reenab the switch to activate all ports as described in [“Enabling and disabling a switch”](#) on page 37.

To unlock a Ports on Demand license, you can use the supplied license key or generate a license key. If you need to generate a key, open an Internet browser and go to the Brocade Web site at www.brocade.com. Click **Products > Software License Keys** and follow the instructions to generate the key.

To enable Ports on Demand

1. Install the Brocade Ports on Demand licensed product. For instructions, see [“Activating a license on a switch”](#) on page 44.
2. Enable the ports as described in [“Enabling and disabling a port”](#) on page 71.

If you remove a Ports on Demand License, the licensed ports are disabled after the next platform reboot or the next port deactivation.

To enable Dynamic Ports on Demand

You must be logged in as Admin to enable or disable the Dynamic PODs feature.

NOTE

The Dynamic PODs feature is supported on the Brocade 4018, 4020, and 4024 switches only. If you click the **Enable DPOD** button on an unsupported switch, an error message displays.

1. Click a port in the Switch View to open the Port Administration window.
2. Click the **FC Ports** or **GigE Ports** tab.
3. From the tree on the left, click the switch or the slot that contains the port.
4. Click the **Enable DPOD** button to enable the licensing mechanism to be dynamic. If the button says **Disable DPOD**, the licensing mechanism is already set to dynamic.

The existing POD associations and assignments are set as the initial Dynamic POD associations.

Two fields are displayed:

- Available Licenses indicate the number of free licenses. These can be allocated for any port.
- Total Licenses indicate the total number of licenses.

To disable Dynamic Ports on Demand

NOTE

Disabling DPODs causes traffic disruption. Any prior port associations and assignments are lost the next time the switch is rebooted.

You must be logged in as Admin to enable or disable the Dynamic PODs feature.

1. Click a port in the Switch View to open the Port Administration window.
2. Click the **FC Ports** or **GigE Ports** tab.
3. From the tree on the left, click the switch or the slot that contains the port.
4. Click the **Disable DPOD** button to set the licensing mechanism to static. If the button displays **Enable DPOD**, the licensing mechanism is already set to static.

Reserving and Releasing Licenses On a Port Basis

You must be logged in as Admin to reserve and release licenses.

NOTE

If the Admin Domains feature is enabled, the Dynamic POD configuration is only applied to the ports if the switch is a member of the current Admin Domain.

The Dynamic PODs feature is supported on the Brocade 4018, 4020, and 4024 switches only.

You must disable the port or switch before reserving or releasing a license.

1. Click a port in the Switch View to open the Port Administration window.
2. Click the **FC Ports** or **GigE Ports** tab.
3. From the tree on the left, click the switch or the slot that contains the port.

The License column identifies the port license status:

- If the port has a license allocated, the License field contains the value Yes.
- If the port does not have a license allocated and there are no free licenses that can be allocated, the License field contains the value No.
- If the port does not have a license allocated and there are licenses that can be allocated to the port, the License field contains the value Possible.

You can reserve or release a license on any port that has a license allocated.

To reserve a license, click **Reserve License** in the Port Administration window.

To release a license, click **Release License** in the Port Administration window.

Swapping port index

If a port malfunctions, or if you want to connect to different devices without having to re-wire your infrastructure, you can move traffic from one port to another (*swap ports*) without changing the I/O Configuration Data Set (IOCDS) on the mainframe computer.

When you perform a port swap, Web Tools automatically disables the two ports, swaps the area IDs, and enables the ports.

To swap ports

1. Click a port in the Switch View to open the Port Administration window.
2. Click the **FC Ports** tab.
3. Click the **Advanced** button.
4. From the tree on the left, select the port you want to swap.
5. Click the **Port Swap** button.
6. Type the number of the port with which you want to swap the current port. If the port is on a blade, you must also provide the slot number.
7. Click **Swap**.

5 Swapping port index

To determine if a port index has been swapped with another switch port

1. Click a port in the Switch View to open the Port Administration window.
2. Click the **FC Ports** tab.
3. Click the **Advanced** button.
4. From the tree on the left, select the port you want to swap.
5. Click the **General** tab.

The *Port Index* attribute in the General tab indicates whether a port has been swapped. For ports that have been swapped, the attribute name displays as *Port Index (Swapped)*, as shown in [Figure 37](#). The value indicates with which port index the port has been swapped.

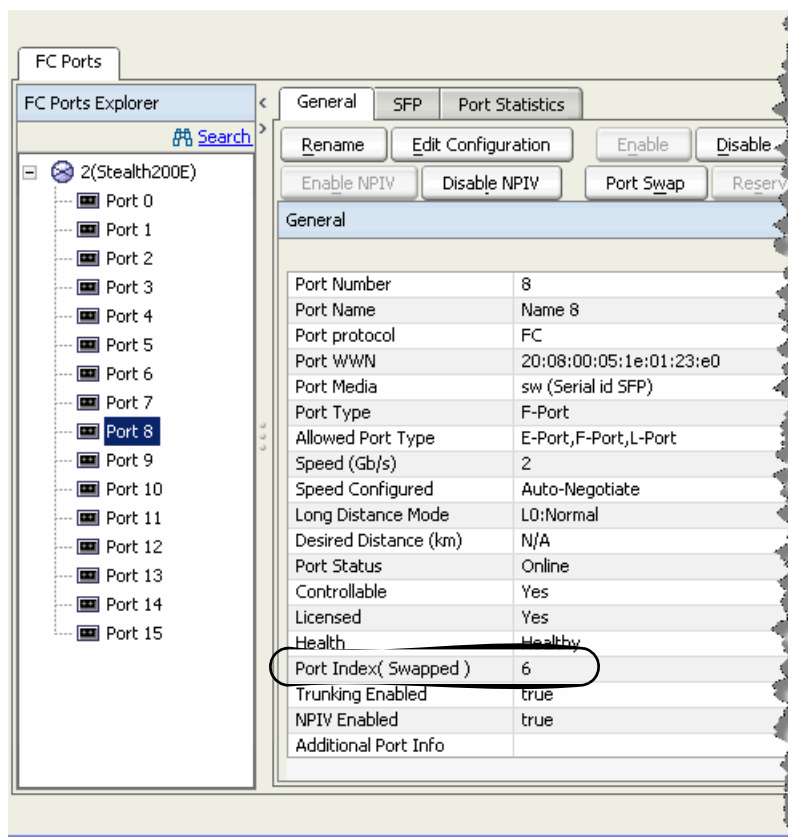


FIGURE 37 Swapping a Port Index

Administering ISL Trunking

In this chapter

This chapter contains the following information:

- [About Interswitch Link Trunking.](#) 77
- [Displaying trunk group information](#) 78
- [Disabling or reenabling trunking mode on a port. . .](#) 78

About Interswitch Link Trunking

Interswitch link (ISL) trunking optimizes network performance by forming trunking groups that can distribute traffic across a shared bandwidth.

A trunking license is required on each switch that participates in the trunk. For details on obtaining and installing licensed features, see [“Managing licensed features”](#) on page 43. For additional information about ISL Trunking, see the *Fabric OS Administrator’s Guide*.

Use the **Trunking** tab of the Switch Administration window to view trunks through Web Tools (see [Figure 38](#)).

6 Displaying trunk group information

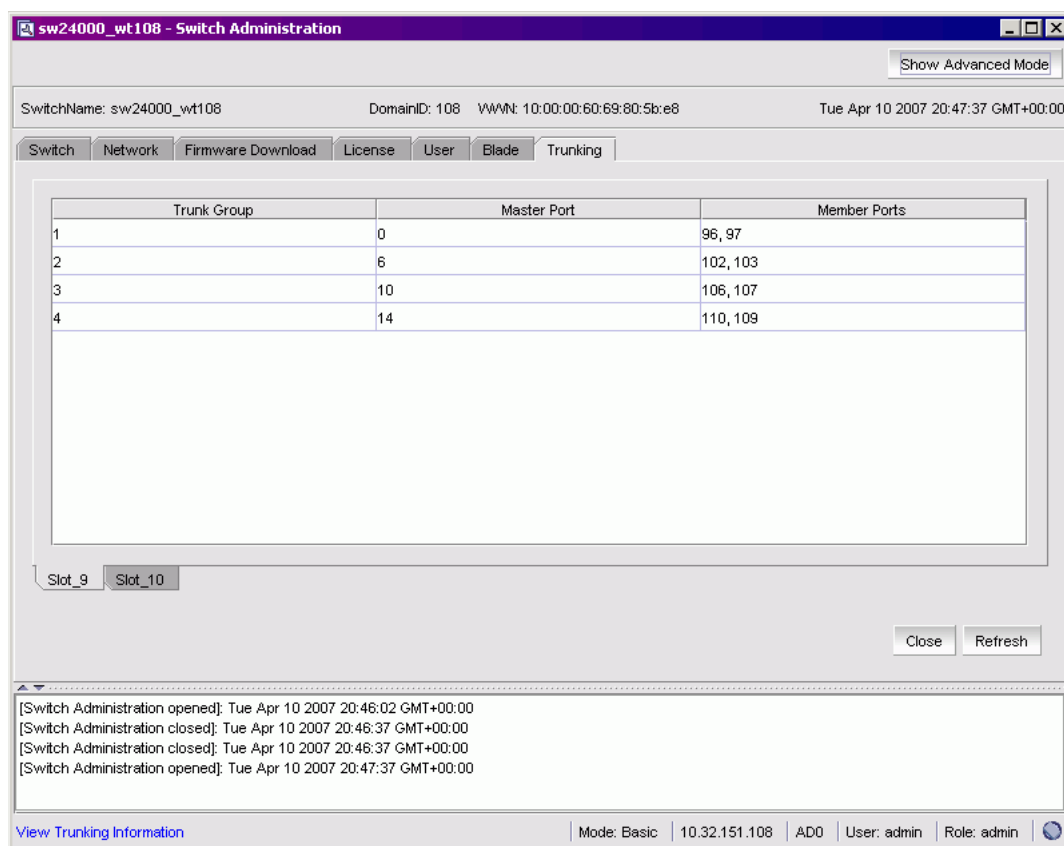


FIGURE 38 Trunking tab

Displaying trunk group information

Use this procedure to display the following information about ISL Trunking groups:

- Trunk group number identifier
- Master port
- Member ports

To view information on a trunk group

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **Trunking** tab.
3. *Optional:* Click **Refresh** to refresh the information.

Disabling or reenabling trunking mode on a port

When the trunking license is activated, trunks are automatically established on eligible ISLs and trunking capability is enabled by default on all ports. Use the following procedure to disable trunking on a port or to reenable trunking if it has been disabled.

Trunking is not supported on logical ports, GbE ports, or EX_Ports.

Admin Domain considerations: You can enable and disable trunking for a port only when the current Admin Domain owns the switch. You can log into a switch that is not in your Admin Domain, but most of the functionality will be unavailable.

To disable or reenable trunking mode on a port

1. Click a port in the Switch View to open the Port Management module (see [Figure 33](#) on page 64).

2. Click the **FC Ports** tab.

Trunking mode does not apply to GbE ports.

3. From the tree on the left, click the switch name or slot name.

4. From the table, select the port that you want to trunk.

You can select multiple ports from the table. You cannot select multiple ports from the tree.

Trunking mode does not apply to logical ports.

5. Click the **Enable Trunking** or **Disable Trunking** button.

If the button is unavailable, the port is already in that state. For example, if **Enable Trunking** is unavailable (appears dimmed), trunking is already enabled for the selected port or ports.

6. Click **Yes** in the confirmation window.

6 Disabling or reenabling trunking mode on a port

Managing Administrative Domains

In this chapter

This chapter contains the following information:

- [About administrative domains](#) 81
- [Implementing administrative domains](#) 83
- [Using the Admin Domain window](#) 84
- [Creating and populating domains](#) 88
- [Managing administrative domains](#) 91

About administrative domains

Using administrative domains (Admin Domains or ADs), you can partition the fabric into logical groups and allocate administration of these groups to different user accounts so that these accounts manage only the Admin Domains assigned to them and do not make changes to the rest of the fabric. The ability to assign an Admin Domain to a specific user account is performed in the User tab of the Switch Administration window and not in the Admin Domain window.

You can create domains that are grouped together based on the type of members in the domain. For example, you can create Admin Domains based on the type of switches in your fabric using the WWN (not to be confused with the Admin Domain number) or put all the devices in a particular department in the same Admin Domain for ease of administering those devices.

You can have up to 256 Admin Domains in a fabric (254 user-defined and 2 system-defined), numbered from 0 through 255. Admin Domains are designated by a name and a number. This document refers to specific Admin Domains using the format “AD n ” where n is a number between 0 and 255.

REQUIREMENTS FOR ADMIN DOMAINS

The following are requirements for using administrative domains:

- Admin Domains are supported on fabrics with switches running Fabric OS 5.2.0 or higher.
- You must have a valid Advanced Zoning license to use Admin Domains.
- A fabric running Fabric OS 5.2.0 or higher with a valid zoning license is called an “AD-capable” fabric.
- To manage Admin Domains, you must be a physical fabric administrator. A physical fabric administrator is a user with the Admin role and access to all Admin Domains (AD0 through AD255).
- The default zone mode setting must be set to No Access (see [“Implementing administrative domains”](#) on page 83).

USER-DEFINED ADMIN DOMAINS

AD1 through AD254 are user-defined Admin Domains. These user-defined Admin Domains can be created only by a physical fabric administrator in AD255.

SYSTEM-DEFINED ADMIN DOMAINS

ADO and AD255 are special Admin Domains and are present in every AD-capable fabric.

ADO

ADO is a system-defined Admin Domain that, in addition to containing members you explicitly added (similar to user-defined Admin Domains), it contains all online devices, switches, and switch ports that have not been assigned to any user-defined Admin Domain.

ADO also implicitly contains all devices from switches running Fabric OS versions earlier than 5.2.0, as they can never be part of an Admin Domain unless and until they are upgraded to v5.2.0.

Unlike user-defined Admin Domains, ADO has an automatic and a fixed membership list. User-defined Admin Domains have only fixed members.

- Automatic membership list—Contains all devices and switches that have not been assigned to any other Admin Domain.
- Fixed membership list—Contains all devices and switches that you explicitly add to ADO and can be used to force device and switch sharing between ADO and other Admin Domains.

The Admin Domain window displays the fixed members and not the automatic members, you can use the View menu to display a list of the automatic members.

ADO can be managed like any user-defined Admin Domain. The only difference between ADO and user-defined Admin Domains is the automatic membership list.

In filtered views, the automatic members of ADO are considered direct members.

The automatic members of ADO change dynamically as the membership of other Admin Domains changes. The fixed members of ADO are not deleted unless you explicitly remove them.

For example, if you explicitly add DeviceA to ADO and it is not a member of any other Admin Domain, then DeviceA is both an automatic and a fixed member of ADO. If you add DeviceA to AD2, then DeviceA is deleted from the ADO automatic membership list, but is *not* deleted from the ADO fixed membership list. If you then remove DeviceA from AD2, DeviceA is added back to the ADO automatic membership list (assuming DeviceA is not in any other Admin Domains).

ADO is useful if you want to share its zone database (called “root zone database”) with a legacy fabric.

AD255 or physical fabric

AD255 is a virtual domain that contains all devices, switches, and switch ports in the fabric. AD255 presents an unfiltered view of the fabric and is also referred to as the physical fabric. The term “physical fabric” is used in Web Tools only.

You can use AD255 to:

- Manage other Admin Domains.
- Get an unfiltered view of the fabric.

- Manage ACL and distribution (can be managed in ADO if no other Admin Domains are present).
- Advanced Performance Monitoring (can be managed in ADO if no other Admin Domains are present).

You cannot manage zones with AD255, because AD255 does not have a zone database associated with it.

ADMIN DOMAIN MEMBERSHIP

Switches, ports, and devices can be members of an Admin Domain. Admin Domain members can be either direct or indirect members.

- Direct members—Devices, switches, and ports that you explicitly add to an Admin Domain. Direct members are listed in the Admin Domain membership list.
- Indirect port members—Ports that are implicitly added as part of an Admin Domain when any of the following occurs:
 - A device that is connected to a port has been added to the Admin Domain.
 - A switch to which the port belongs is a member of the Admin Domain.
- Indirect device members—Devices that are connected to ports that are direct members of an Admin Domain.

Implementing administrative domains

The default zone mode setting gives your attached devices either All Access to all devices or No Access to all devices. To begin implementing an Admin Domain structure within a SAN, you must set the default zone mode to No Access. You must be in ADO to change the default zone mode. *After the default zone mode has been set to No Access, you cannot change it from the physical fabric.*

Even though the default zone mode access is set to No Access, you can still create and enable zones within each Admin Domain. These zones are configurable only from the Admin Domain in which they were created. Indirect port members cannot be zoned.

To enable Admin Domains

1. Change the Admin Domain context to ADO. See [“Admin Domain Context”](#) on page 20.
2. Change the Default Zone mode to No Access. See [“Setting the default zoning mode”](#) on page 97.
3. Navigate to AD255 or the physical fabric and begin managing the Admin Domains.

Using the Admin Domain window

You can view and manage Admin Domains through the Admin Domain window, shown in [Figure 39](#). You access the Admin Domain window by clicking Admin Domain in the Manage section of the Tasks menu.

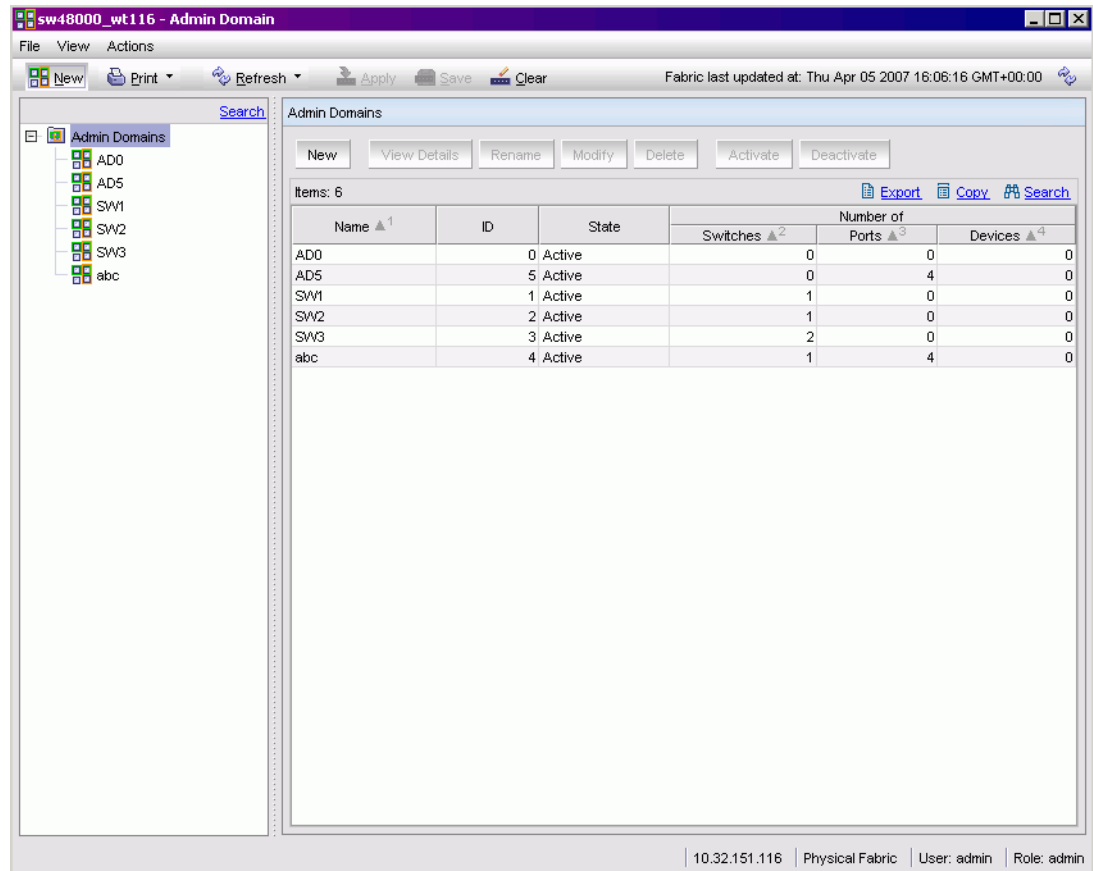


FIGURE 39 Admin Domain window, summary view

The Admin Domain window displays information about the Admin Domains defined in the fabric. If you launch the Admin Domain window from AD255 (physical fabric), the window contains information about the current content of all Admin Domains. If you launch the Admin Domain window from any other Admin Domain, the module displays the current Admin Domain only.

To manage Admin Domains, you must be logged in with the role of Admin.

ATTENTION

Any changes you make in the Admin Domain window are held in a buffered environment and are *not saved to persistent storage until you explicitly save the changes*. If you close the Admin Domain window without saving your changes, your changes are lost. To save the buffered changes you make in the Admin Domain window to persistent storage, see [“Saving local admin domain changes”](#) on page 87.

When you are logged into ADO, if a physical fabric administrator modifies the AD configuration from another session, the changes in the membership might not be visible to you.

When you launch the Admin Domain window and select the parent **Admin Domains** node in the tree on the left side of the module, the Admin Domain window displays summary information about all of the Admin Domains, as shown in [Figure 39](#). You can also select a specific Admin Domain from the tree to display detailed information about that Admin Domain, as shown in [Figure 40](#). The detailed view displays summary information as well as information about the online switch, port, and device members of the selected Admin Domain.

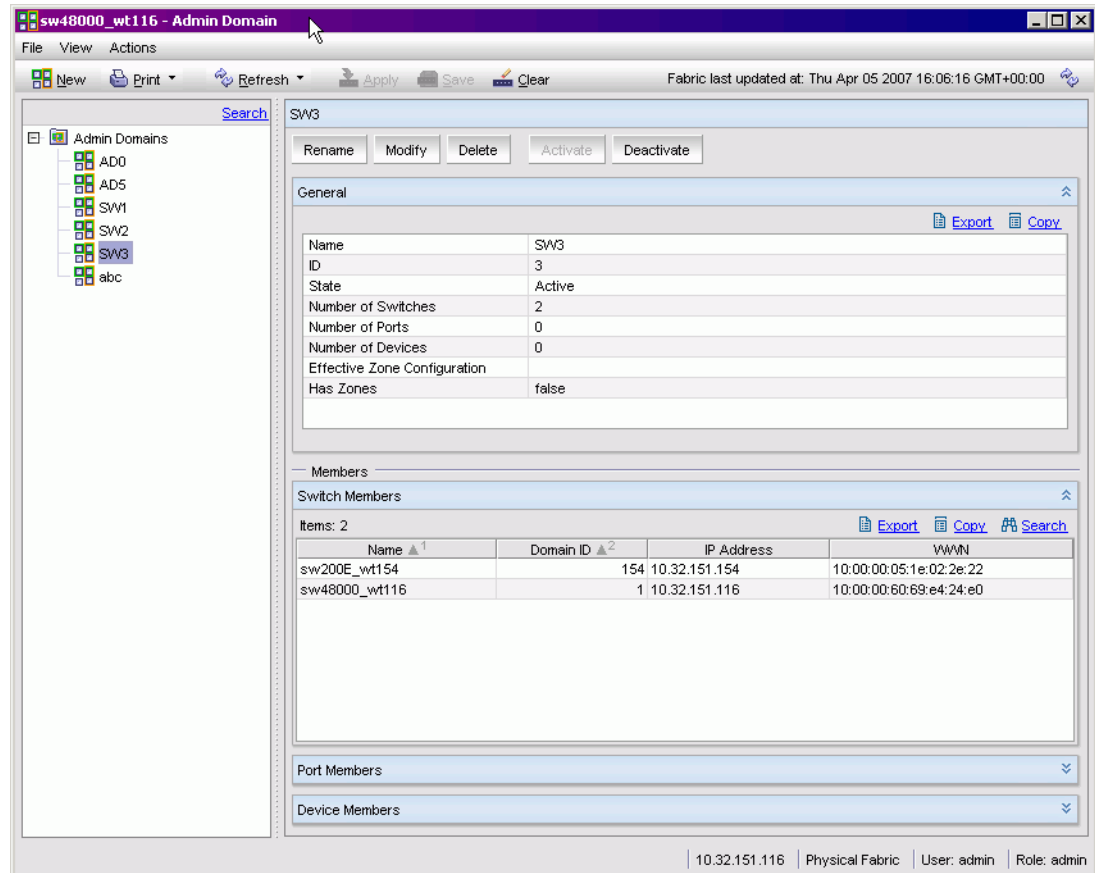


FIGURE 40 Admin Domain window, single admin domain detail

The Admin Domain window has buttons in a task bar at the top of the window:

- **New** lets you create a new Admin Domain.
- **Print** lets you print the current or effective configuration.
- **Refresh** lets you refresh the information for the entire fabric or a specific Admin Domain.
- **Apply** lets you apply a configuration.
- **Save** lets you save a configuration.
- **Clear** lets you clear the configuration.

The Admin Domain window also contains **Export**, **Copy**, and **Search** links at the top of the each table. The options are not available if the table does not have any content.

NOTE

You must accept the Brocade Certificate at the beginning of the login to Web Tools to enable the functionality of Export and Copy.

- Click **Export** to save the contents of the table to a tab-delimited file.
- Click **Copy** to copy the contents of the table in tab-delimited text format to a file.
- Click **Search** to search for a specific text string in the table.

A pop-up box appears, as shown in [Figure 41](#).

In the pop-up box, type the text string and press **Enter**. This is an incremental search and allows 24 maximum characters including the wildcards question mark (?) and asterisk (*). The first row containing the text string is highlighted. To find the next match, press the down arrow. To find the previous match, press the up arrow. If the text is not found in the table, the text turns red.

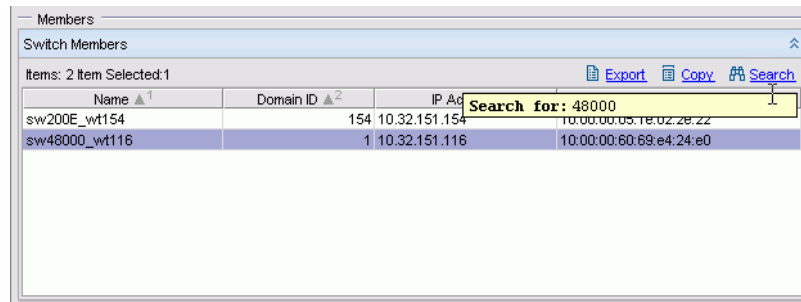


FIGURE 41 Search for a text string in a table

OPENING THE ADMIN DOMAIN WINDOW

This section describes how to open the Admin Domain window. You use the Admin Domain window to perform all Admin Domain configuration procedures.

If you want to configure Admin Domains, you must launch the Admin Domain window from the physical fabric context. If you are in any Admin Domain other than the physical fabric, the module launches in read-only mode.

To open the Admin Domain window

1. Select a switch from the Fabric Tree and log in when prompted. The switch must be running Fabric OS 5.2.0 or higher.

Switch View displays information for the selected switch.

2. If you plan to modify the Admin Domain configuration, from the **Admin Domain** drop-down menu, select **Physical Fabric**.
3. Click **Admin Domain** in the **Manage** section of the **Tasks** menu.

The Admin Domain window opens (see [Figure 39](#)).

REFRESHING FABRIC INFORMATION

This function refreshes the display of *fabric elements only* (switches, ports, and devices). It does not update Admin Domain changes in the Admin Domain window. To refresh the Admin Domain information, see [“Refreshing admin domain information,”](#) next.

This option allows you to refresh the fabric element information displayed at any time.

To refresh the fabric information

1. In the Admin Domain window, click **Refresh**.

This refreshes the status for the fabric, including switches, ports, and devices.

REFRESHING ADMIN DOMAIN INFORMATION

Any changes you make to the Admin Domain window are saved to a local buffer; they are not applied to persistent storage until you invoke one of the transactional operations listed in the **Actions** menu.

You can refresh the Admin Domain information at any time to reflect changes that might have been made by other users or to back out of current, unsaved work and start again.

ATTENTION

When you refresh the buffered information in the Admin Domain window, any Admin Domain configuration changes you have made *and not yet saved* are erased from the buffer and replaced with the currently enabled zone Admin Domain information that is saved on the switch.

The following procedure updates the information in the Admin Domain window with the information saved on the switch.

To refresh the local Admin Domain buffer from the saved configuration

1. In the Admin Domain window, click the drop-down arrow on the **Refresh button**, and then click **Refresh Admin Domains**.

This refreshes the information in the Admin Domain window with the saved information on the switch. This action also refreshes the fabric information as described in [“Refreshing fabric information”](#) on page 87. Any unsaved Admin Domain changes are deleted.

SAVING LOCAL ADMIN DOMAIN CHANGES

All information displayed and all changes made in the Admin Domain window are buffered until you save the changes. That means that any other user looking at the Admin Domain information for the switch will not see the changes you have made until you save them.

Click **Actions> Save AD Configuration** to save your changes to persistent storage as the defined Admin Domain configuration. Click **Actions> Apply AD Configuration** to save your changes to persistent storage *and make your changes effective in the fabric*. These options are not enabled until you make a change to the Admin Domain configuration.

If another user has an Admin Domain operation in progress at the time that you attempt to save changes, Web Tools displays a warning to indicate that another Admin Domain transaction is in progress on the fabric. You can select to abort the other transaction and override it with yours.

This action updates the entire contents of the Admin Domain window, not just the selected Admin Domain. You can save your changes at any time during the Admin Domain configuration session.

CLOSING THE ADMIN DOMAIN WINDOW

It is very important to remember that any changes you make in the Admin Domain window are not saved automatically.

To close the Admin Domain window

1. From the Admin Domain window, click **File > Close**.
If there are changes in the buffer that have not been saved, a warning appears. Confirm that you want to close the Admin Domain session without saving the changes.
2. Click **Yes** to close without saving changes or click **No** to go back to the Admin Domain window to save the changes (see [“Saving local admin domain changes”](#) on page 87).

Creating and populating domains

Setting up an Admin Domain involves the following steps:

1. Create and activate an Admin Domain.
2. Assign one or more administrators to the Admin Domain. The Admin account always has access to administer the Admin Domains, even if no other users are assigned (see [“Changing Account Parameters”](#) on page 205).

When you create an Admin Domain, you can activate the Admin Domain after you finish creating it. If you activate the Admin Domain, you must click **Apply** to transfer your changes from the Web Tools database to the fabric database so that your changes are applied to the fabric.

You can log in to an active Admin Domain. You cannot log in to an Admin Domain that has been deactivated.

The following procedures provide detailed instructions for creating an Admin Domain and for activating or deactivating an existing Admin Domain.

To create an Admin Domain

1. Open the Admin Domain window as described on [page 86](#).
2. Click **New**.

The Create Admin Domain wizard opens.

FIGURE 42 Create Admin Domain wizard

3. In the Name area, assign an Admin Domain name.
You can specify a name or let the system assign the name for you.
4. In the ID area, assign an Admin Domain ID.
You can specify an ID or let the system assign the ID for you.
5. In the State area, select the **Active** check box to activate the Admin Domain when you finish creating it. This is the default setting.
Clear the **Active** check box if you want the Admin Domain deactivated when you finish creating it.
6. Click **Next**.
7. In the Membership area, assign members to the Admin Domain by selecting them in the Available Members section and clicking **Add**, **Add Ports**, or **Add Devices**.
 - Select a switch, port, or device in the Available Members tree and click **Add** to add the selected element.
Alternatively, you can press the **Insert** key to add your selections.
 - Select a switch or slot and click **Add Ports** to add all of the ports in the selected switch or slot.
 - Select a switch, slot, or port and click **Add Devices** to add all of the devices for the selected element.

Optional: Click the **Manual** button to add offline devices.

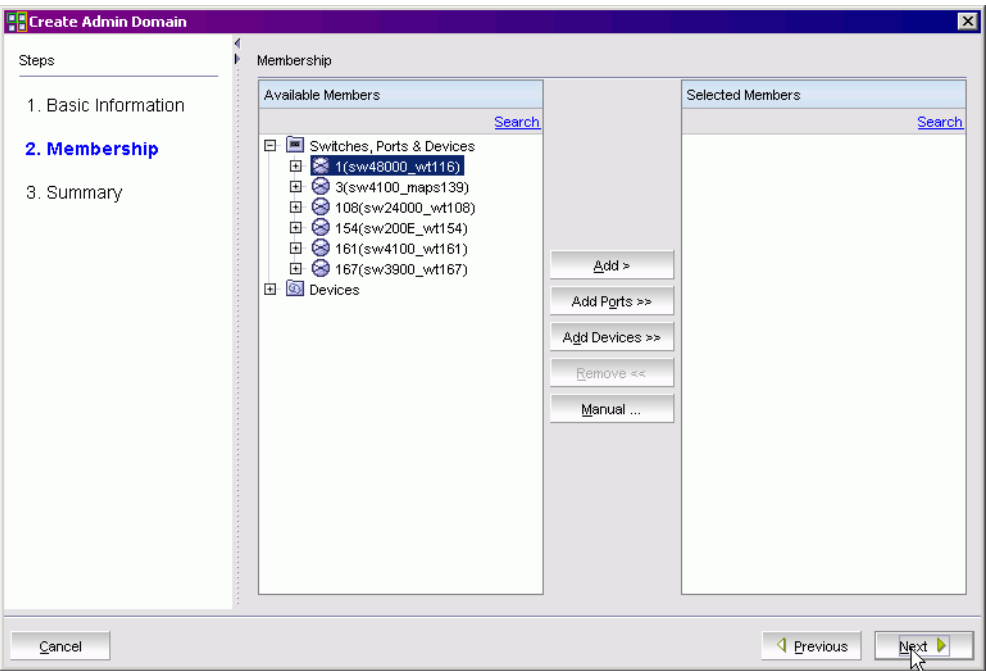


FIGURE 43 Adding members to an Admin Domain

8. Click **Next**.

The wizard displays a summary of the Admin Domain. Read the summary to verify the Admin Domain setup is correct.

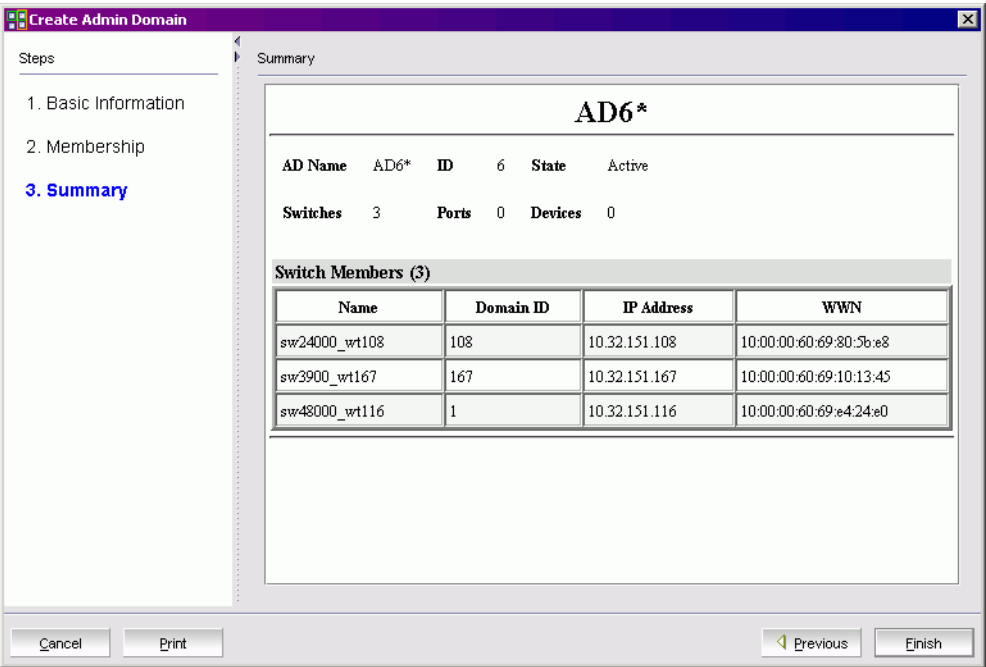


FIGURE 44 Summary view

9. Click **Finish** to close the wizard.
10. Click **Save** to save the new Admin Domain configuration to persistent storage.
11. Click **Apply** to enforce the new Admin Domain configuration as the effective configuration.

To activate or deactivate an Admin Domain

1. Open the Admin Domain window.
2. From the tree on the left, select the Admin Domain you want to activate or deactivate.
3. Click the **Activate** button to activate the Admin Domain.
Click the **Deactivate** button to deactivate the Admin Domain.
4. Click **Actions> Save AD Configuration** to save the new Admin Domain configuration to persistent storage.
5. Click **Actions> Apply AD Configuration** to enforce the new Admin Domain configuration as the effective configuration.

ATTENTION

When you deactivate an Admin Domain, the members or devices assigned to the domain can no longer access their hosts or storage unless those devices are part of another Admin Domain.

When you deactivate an Admin Domain no one can use this Admin Domain to log in to a switch.

Managing administrative domains

This section provide information on how to manage Admin Domains after they have been created.

ADDING AND REMOVING MEMBERS

The only thing you can edit when you modify the Admin Domain is the membership. Use the following procedure to add or remove members from an Admin Domain.

To modify the members of a domain

1. Open the Admin Domain window.
2. From the tree on the left, select the Admin Domain you want to modify.
3. Click **Modify**.

The Modify Admin Domain wizard opens on the Membership step.

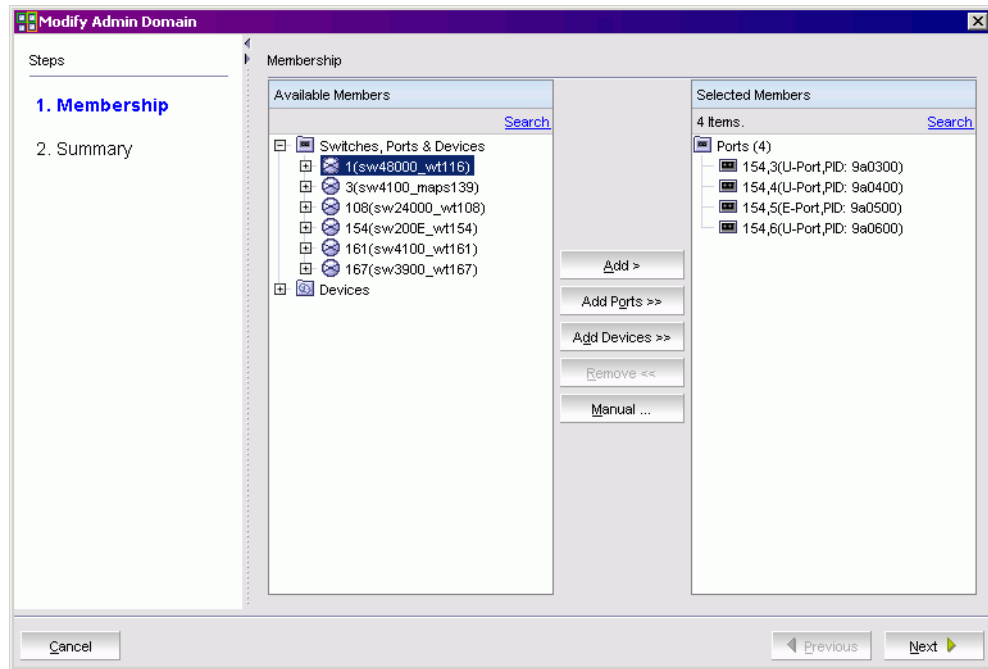


FIGURE 45 Modify Admin Domain wizard

4. Assign members to the Admin Domain by selecting them in the Available Members section and clicking **Add**, **Add Ports**, or **Add Devices**.
 - Select a switch, port, or device in the Available Members tree and click **Add** to add the selected element.
Alternatively, you can press the **Insert** key to add your selections.
 - Select a switch or slot and click **Add Ports** to add all of the ports in the selected switch or slot.
 - Select a switch, slot, or port and click **Add Devices** to add all of the devices for the selected element.
Optional: Click **Manual** to add offline switches and devices.
5. Remove members from the Admin Domain by selecting them in the Selected Members section and clicking **Remove**.
Alternatively, you can press the **Delete** key to remove selected items.
6. Click **Next**.
Use the summary to verify that the Admin Domain setup is correct.
7. Click **Finish**.
8. Click **Actions> Save AD Configuration** to save the new Admin Domain configuration to persistent storage.
9. Click **Actions> Apply AD Configuration** to enforce the new Admin Domain configuration as the effective configuration.

RENAMING ADMIN DOMAINS

You can change the name of an Admin Domain, including an auto-assigned ID name.

The Admin Domain name cannot exceed 63 chars and can contain alphabetic and numeric characters. The only special character allowed is an underscore (_).

NOTE

You cannot rename ADO or AD255.

To rename a domain

1. Open the Admin Domain window.
2. From the tree on the left, select the Admin Domain.
3. Click the **Rename** button.
4. Enter the new name.
5. Click **OK**.
6. Click **Actions> Save AD Configuration** to save the new Admin Domain configuration to persistent storage.
7. Click **Actions> Apply AD Configuration** to enforce the new Admin Domain configuration as the effective configuration.

DELETING ADMIN DOMAINS

When you delete an Admin Domain its devices no longer have access to the members of the zones with which it was associated.

To delete a domain

1. Open the Admin Domain window.
2. From the tree on the left, select the Admin Domain.
3. Click **Delete**.
4. In the confirmation box, click **Yes** to delete the domain.
The system deletes the Admin Domain.
5. Click **Actions> Save AD Configuration** to save the new Admin Domain configuration to persistent storage.
6. Click **Actions> Apply AD Configuration** to enforce the new Admin Domain configuration as the effective configuration.

Deleting all user-defined Admin Domains

When you clear the Admin Domain configuration, all user-defined Admin Domains are deleted and all fabric resources (switches, ports, and devices) are returned to ADO.

You cannot clear the Admin Domain configuration if zone configurations exist in any of the user-defined Admin Domains.

7 Managing administrative domains

To clear the entire Admin Domain configuration

1. Open the Admin Domain window.
2. Click **Actions> Clear AD Configuration**.
3. In the confirmation dialog box, click **Yes** to clear the Admin Domain configuration.
Click **No** to cancel the action.

Administering Zoning

This chapter briefly describes zoning and provides the procedures for managing zoning using Brocade Web Tools. It contains the following sections:

In this chapter

- [Introducing zoning](#) 95
- [Configuring zoning](#) 96
- [Managing zoning with Web Tools](#) 97
- [Managing zone aliases](#) 102
- [Managing zones](#) 104
- [Managing zone configurations](#) 106
- [Managing the zoning database](#) 114
- [Best practices for zoning](#) 119

Introducing zoning

Zoning enables you to partition a storage area network (SAN) into logical groups of devices that can access each other. For example, you can partition a SAN into two zones, *winzone* and *unixzone*, so that the Windows servers and storage do not interact with UNIX servers and storage.

Zones can be configured dynamically. They can vary in size, depending on the number of fabric-connected devices, and devices can belong to more than one zone. Because zone members can access only other members of the same zone, a device not included in a zone is not available to members of that zone.

When using a mixed fabric—that is, a fabric containing two or more switches running different fabric operating systems—you should use the switch with the highest Fabric OS level to perform zoning tasks. See [“Best practices for zoning”](#) on page 119 for more recommendations about zoning.

When zone or Fabric Assist (FA) zone members *are specified by fabric location only* (domain, area), or *by device name only* (node name or port WWN), zone boundaries are enforced at the hardware level and the zone is referred to as a “hard zone.”

When zone members are specified by fabric location (domain, area) *and other members of the same zone* are specified by device name (node name or port WWN), zone enforcement depends on Name Server lookups, and the zone is referred to as a “soft zone.”

For more specific information about zoning concepts, see the *Fabric OS Administrator's Guide*.

Zoning and admin domains

Each admin domain has its own zone database, with both defined and effective zone configurations and all related zone objects (zones, zone aliases, and zone members). Within an admin domain, you can configure zoning only with the devices that are present in that admin domain (direct members).

If you upgrade a fabric to Fabric OS 5.2.0 or higher, the zone database from the pre-v5.2.0 fabric is referred to as the “root zone database” and is owned by ADO.

Each zone database has its own namespace; for example, the zone name *test_z1* can be defined in more than one admin domain.

No zone databases are linked to the physical fabric (AD255). The only zone operation supported from AD255 is viewing the complete hierarchical zone database (zone databases of ADO through AD254) using the command line interface. See the *Fabric OS Administrator's Guide* for additional information.

If you implement admin domains, the default zoning mode must be set to No Access before you create admin domains. See [“Setting the default zoning mode”](#) on page 97.

See [page 99](#) for additional information about how admin domains affect zoning.

Configuring zoning

This section outlines the basic steps for configuring zoning as shown below.

- [“Creating and populating zone aliases”](#) on page 102
- [“Creating and populating zones”](#) on page 104
- [“Creating zone configurations”](#) on page 107
- [“Saving local zoning changes”](#) on page 100
- [“Enabling zone configurations”](#) on page 109

The next section describes the Zone Administration window, in which all of the zoning tasks are performed. The remainder of this chapter provides procedures for managing zones, zone aliases, zone configurations, and zone server information.

OPENING THE ZONE ADMINISTRATION WINDOW

This section describes how to launch the Zone Administration window, from which all zoning procedures are performed. You cannot open the Zone Administration window from AD255 (physical fabric).

To open the Zone Administration window

1. Select a switch from the [Fabric Tree](#).
2. Click **Zone Admin** in the **Manage** section of the **Tasks** menu.

The Zone Administration window opens (see [Figure 46](#)).

SETTING THE DEFAULT ZONING MODE

The default zoning mode defines the device accessibility behavior if zoning is not implemented or if there is no effective zone configuration. The default zoning mode has two options:

- All Access—All devices within the fabric can communicate with all other devices.
- No Access—Devices in the fabric cannot access any other device in the fabric.

Web Tools supports default zoning on switches running firmware v5.1.0 or higher. Default zoning on legacy switches (switches running firmware versions prior to v 5.1.0) are not supported. Legacy switches can use default zoning; however, they cannot manipulate the default zone or default configuration.

NOTE

If you want to use Admin Domains, you must set the default zoning mode to No Access prior to setting up the Admin Domains. You cannot change the default zoning mode to All Access if user-specified Admin Domains are present in the fabric.

To set the default zone mode

1. Open the Zone Administration window (see [“Opening the Zone Administration window”](#) on page 96).
2. Click **Zoning Actions> Set Default Mode**, and then select the access mode.

Managing zoning with Web Tools

You can monitor and manage zoning through the Web Tools Zone Administration. Click Zone Admin to access the Zone Administration window, shown in [Figure 46](#). Zone Administration appears only if an Advanced Zoning license is installed on the switch.

The information in the Zone Administration window is collected from the selected switch.

If secure mode is enabled, zoning can be administered only from the primary FCS switch. If the selected switch has an Advanced Zoning license installed but is not the primary FCS switch, the Zone Admin option is displayed but not activated. For specific information on secure fabrics, see the *Secure Fabric OS Administrator's Guide*.

You must be logged into the switch using a user name with one of the following roles associated with it to make changes to the zoning: zoneAdmin, admin, or fabricAdmin. All other roles allow only a view or read-only access. Most of the zoning operations are disabled in read-only mode.

A snapshot is taken of all the zoning configurations at the time you launch the Zone Administration window; this information *is not updated automatically* by Web Tools. To update this information, see [“Refreshing Zone Administration window Information”](#) on page 99.

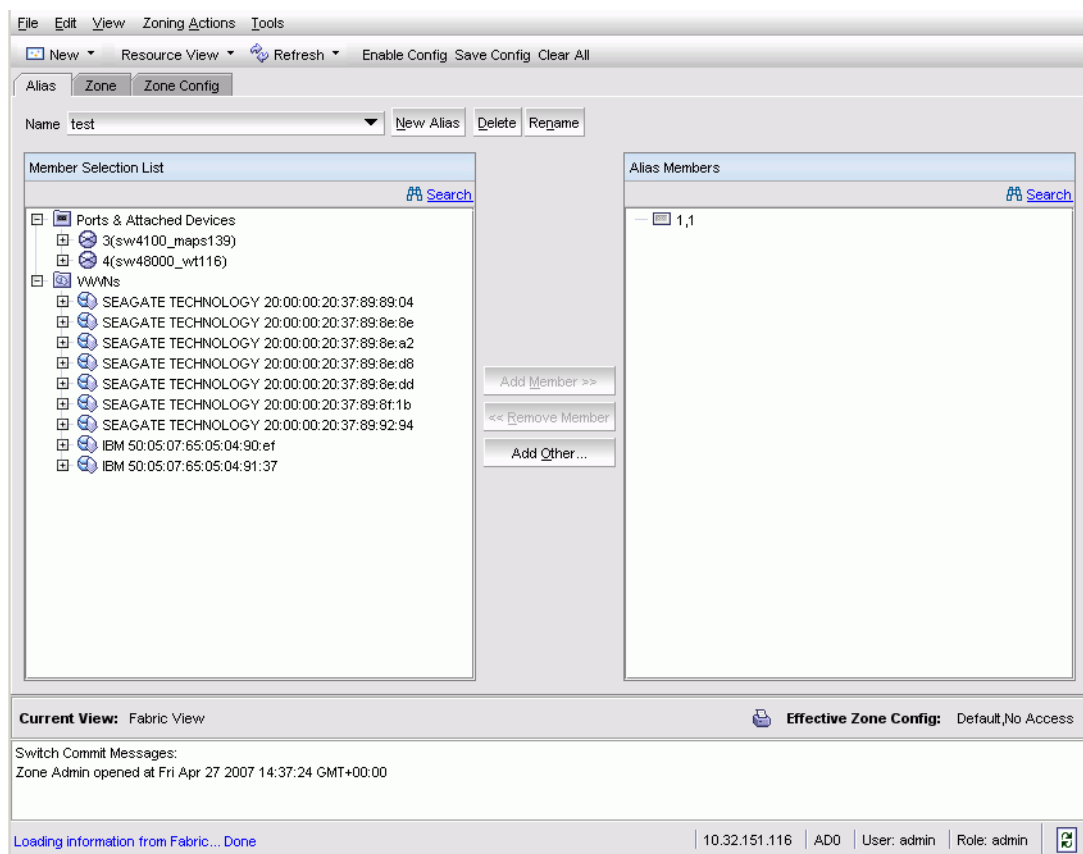


FIGURE 46 Zone Administration window

ATTENTION

Any changes you make in the Zone Administration window are held in a buffered environment and *are not updated in the zoning database until you save the changes*. If you close the Zone Administration window without saving your changes, your changes are lost. To save the buffered changes you make in the Zone Administration window to the zoning database on the switch, see [“Saving local zoning changes”](#) on page 100.

Note the following:

- “Saving” means updating the zoning database on the switch with the local changes from the Web Tools buffer.
- “Refreshing” means copying the current state of the zoning database on the switch to the Web Tools buffer, overwriting its current contents.

In the Zone Administration window, all WWNs also display vendor names. In the Member Selection List panel (see [Figure 46](#)), you can right-click port and device nodes to display which aliases the port or device is a member of. In addition, you can right-click the device nodes and click **View Device Detail** to display detailed information about the selected device.

The Member Selection List panel displays both physical and logical FC ports; however, GbE ports are not supported for zoning. To verify whether you have any unzoned devices, analyze the current configuration for unzoned and offline devices (for more information see [“Creating configuration analysis reports”](#) on page 113).

The Member Selection List displays virtual initiators if the chassis has an FC4-16IP blade in it; they are shown under a separate folder icon called Virtual Initiators.

Admin Domain considerations: The Member Selection List panel displays a filtered list of ports.

- Direct port members are zoneable and are displayed in the tree.
- Indirect port members to which owned devices are attached are displayed in the tree, but cannot be added to a zone or alias.
- Direct device members are zoneable and are displayed in the tree.
- Indirect device members (devices that are currently attached to owned ports) are also zoneable and displayed in the tree. But if such a device is later moved to a non-owned port it will no longer be displayed or zoneable.
- Switches and blades are displayed only if they contain owned ports or devices, regardless of switch ownership.
- Ports that are indirect members only because the switch is owned *are not displayed*.

The remainder of this section describes basic zoning procedures you can perform in the Zone Administration window, which are also useful for all zoning operations.

REFRESHING FABRIC INFORMATION

This function refreshes the display of *fabric elements only* (switches, ports, and devices). It does not affect any zoning element changes or update zone information in the Zone Administration window. To refresh the zone information displayed in the Zone Administration window, see [“Refreshing Zone Administration window Information,”](#) next. You can refresh the fabric element information displayed at any time.

To refresh fabric information

1. In the Zone Administration window, click **View> Refresh From Live Fabric**.

This refreshes the status for the fabric, including switches, ports, and devices.

NOTE

Depending on the role associated with your user name or if the switch is owned by the current Admin Domain you are logged in to, you may not be able to modify zones or ports in other Admin Domains.

REFRESHING ZONE ADMINISTRATION WINDOW INFORMATION

The information displayed in the Zone Administration window is initially a snapshot of the contents of the fabric zoning database at the time the window is launched. Any changes you make to this window are saved to a local buffer; but they are not applied to the fabric zoning database until you invoke one of the transactional operations listed in the Zoning Actions menu.

Any local zoning changes are buffered by the Zone Administration window until explicitly saved to the fabric. If the fabric zoning database is independently changed by another user or from another interface (for example, the CLI) while Web Tools zoning changes are still pending, the refresh icon starts to blink (after a 15–30 second polling delay). You can then choose to refresh the current Web Tools zoning view to reflect the new, externally changed contents of the fabric zoning database, in which case any pending local changes are lost, or you can ignore the blinking refresh icon and save your local changes, overwriting the external changes that triggered the icon to blink.

You can refresh zoning to back out current, unsaved work and start over.

You can refresh the zoning information at any time, either using the refresh icon (whether it is flashing or not) or from the View menu.

The following procedure updates the information in the Zone Administration window with the information saved in the zoning database on the switch.

ATTENTION

When you refresh the buffered information in the Zone Administration window, any zoning configuration changes you have made *and not yet saved* are erased from the buffer and replaced with the currently enabled zone configuration information that is saved on the switch.

To refresh the local Zone Admin buffer from the fabric zoning database

1. Launch the Zone Administration window as described on [page 96](#).
2. Click **View> Refresh Zoning** or click the Refresh button.

This refreshes the information in the Zone Administration window with the information in the switch's zoning database. This action also refreshes the fabric information as described in "[Refreshing fabric iNformation](#)" on page 99. Any unsaved zoning changes are deleted.

SAVING LOCAL ZONING CHANGES

All information displayed and all changes made in the Zone Administration window are buffered until you save the changes. That means that any other user looking at the zone information for the switch will not see the changes you have made until you save them.

Saving the changes propagates any changes you have made in the Zone Administration window (buffered changes) to the zoning database on the switch. If another user has a zoning operation in progress at the time that you attempt to save changes, a warning is displayed that indicates that another zoning transaction is in progress on the fabric. You can select to abort the other transaction and override it with yours.

If the zoning database size exceeds the maximum allowed, you cannot save the changes. The zoning database summary displays the maximum zoning database size (see "[Displaying zone configuration summaries](#)" on page 112).

This action updates the entire contents of the Zone Administration window, not just the selected zone, alias, or configuration. You can save your changes at any time during the Zone Administration session.

To save zone changes to the switch zoning database

1. Make the zoning changes in the Zone Administration window.
2. Click **Zoning Actions> Save Config Only**.

NOTE

If you have made changes to a configuration, you must enable the configuration before the changes will be effective. To enable the configuration, see [“Enabling zone configurations”](#) on page 109.

CLOSING THE ZONE ADMINISTRATION WINDOW

It is very important to remember that any changes you make in the Zone Administration window are not saved automatically. It is recommended that you always close the Zone Administration window from the **File** menu, as described in the procedure below.

ATTENTION

When you click the X in the upper-right corner of the Zone Administration window, the session is closed without any warning messages about unsaved changes. To avoid potential loss of data, use the following procedure to close the Zone Administration window. In this procedure, the system displays a warning if you have unsaved changes when you are trying to close the Zone Administration window.

To safely close the Zone Administration window

1. From the Zone Administration window, click **File> Close**.

If any changes exist in the buffer that have not been saved, a warning message dialog box provides you with the option of saving your changes.
2. Click **Yes** to close without saving changes, or click **No** to go back to the Zone Administration window to save the changes as described in [“Saving local zoning changes”](#) on page 100.

ZONING VIEWS

You can choose how zoning elements are displayed in the Zone Administration window. The zoning view you select determines how members are displayed in the Member Selection List panel (see [Figure 46](#)). The views filter the fabric and device information displayed in the Member Selection List for the selected view, making it easier for you to create and modify zones, especially when creating “hard zones.”

Depending on the method you use to zone, certain tabs might or might not be available in the Zone Administration window.

There are two views of defining members for zoning:

- **Fabric View**—Displays the physical hierarchy of the fabric, a list of the attached and imported physical devices (by WWN), and a list of the FC Virtual Initiators on switches that support iSCSI. In the Fabric View, you can select ports for port-based zoning or devices for WWN-based zoning.
- **Devices Only**—Displays a list of the attached and imported physical devices by WWN. You cannot select ports for port-based or mixed zoning schemes, nor can you select virtual initiators for iSCSI FC Zone creation.

To select a zoning view

1. Launch the Zone Administration window as described on [page 96](#).
2. Click **View> Choose Fabric Resources View**.
3. Choose the way you want to view the fabric resource and click **OK**.

Managing zone aliases

An alias is a logical group of port index numbers and WWNs. Specifying groups of ports or devices as an alias makes zone configuration easier, by enabling you to configure zones using an alias rather than inputting a long string of individual members. You can specify members of an alias using the following methods:

- A switch domain and port index number pair, for example, 2, 20
- Device node and device port WWNs

CREATING AND POPULATING ZONE ALIASES

Use the following procedure to create a zone alias.

To create a zone alias

1. Open the Zone Administration window as described on [page 96](#).
2. Select a format to display zoning members in the Member Selection List as described in [“Zoning views”](#) on page 101.
3. Click the **Alias** tab and click **New Alias**.
The Create New Alias dialog box displays.
4. On Create New Alias, type a name for the new alias and click **OK**.
The new alias is displayed in the Name drop-down list.
5. Expand the Member Selection List to view the nested elements.
The choices available in the Member Selection List depend on the selection in the View menu.
6. Click elements in the Member Selection List that you want to include in the alias.
The **Add Member** button becomes active.
7. Click **Add Member** to add alias members.
Selected members move to the Alias Members window.
8. *Optional:* Repeat steps 6 and 7 to add more elements to the alias.
9. *Optional:* Click **Add Other** to include a WWN or port that is not currently a part of the fabric.
10. *Optional:* Click **Add Other Host** to include a WWN or port that is not currently a part of the fabric.
At this point you can either save your changes or save and enable your changes.
11. Click **Actions> Save Config Only** to save the configuration changes.
To enable the configuration, see [“Enabling zone configurations”](#) on page 109.

ADDING AND REMOVING MEMBERS OF A ZONE ALIAS

Use the following procedure to add or remove zone alias members.

To modify the members of an alias

1. Open the Zone Administration window as described on [page 96](#).
2. Click the **Alias** tab.
3. Select the alias you want to modify from the Name drop-down list.
4. Select an element in the **Member Selection List** that you want to add to the alias, or select an element in the **Alias Members** list that you want to remove.
5. Click **Add Member** to add the selected alias member, or click **Remove Member** to remove the selected alias member.

The alias is modified in the Zone Admin buffer. At this point you can either save your changes or save and enable your changes.

6. Click **Zoning Actions> Save Config Only** to save the configuration changes.

To enable the configuration, see [“Enabling zone configurations”](#) on page 109.

RENAMING ZONE ALIASES

Use the following procedure to change the name of a zone alias.

To rename a zone alias

1. Open the Zone Administration window as described on [page 96](#).
2. Click the **Alias** tab and select the alias you want to rename from the Name drop-down list.
3. Click **Rename**.

The Rename an Alias dialog box appears.

4. Type a new alias name and click **OK**.

The alias is renamed in the Zone Admin buffer. At this point you can either save your changes or save and enable your changes.

5. Click **Zoning Actions> Save Config Only** to save the configuration changes.

To enable the configuration, see [“Enabling zone configurations”](#) on page 109.

DELETING ZONE ALIASES

You can remove a zone alias from the Zone Admin buffer. When a zone alias is deleted, it is no longer a member of the zones of which it was once a member.

To delete a zone alias

1. Open the Zone Administration window as described on [page 96](#).
2. Click the **Alias** tab.
3. Select the alias you want to delete from the Name drop-down list.
4. Click **Delete**.

The Confirm Deleting Alias dialog box displays.

5. Click **Yes**.

The selected alias is deleted from the Zone Admin buffer. At this point you can either save your changes or save and enable your changes.

6. Click **Zoning Actions** > **Save Config Only** to save the configuration changes.

To enable the configuration, see [“Enabling zone configurations”](#) on page 109.

Managing zones

A zone is a region within the fabric in which specified switches and devices can communicate. A device can communicate only with other devices connected to the fabric within its specified zone. You can specify members of a zone using the following methods:

- Alias names
- Switch domain and port index number pair, for example, 2, 20
- WWN (device)

CREATING AND POPULATING ZONES

Use the following procedure to create a zone.

To create a zone

1. Open the Zone Administration window as described on [page 96](#).
2. Select a format to display zoning members in the Member Selection List as described in [“Zoning views”](#) on page 101.

3. Click the **Zone** tab.

4. Click **New Zone**.

The Create New Zone dialog box displays.

5. On Create New Zone, enter a name for the new zone, and click **OK**.

If you are creating an LSAN zone, the zone name must begin with “LSAN_”.

The new zone appears in the Name drop-down list.

6. Expand the Member Selection List to view the nested elements.

The choices available in the list depend on the selection made in the View menu.

7. Select an element in the Member Selection List that you want to include in your zone. Note that LSAN zones should contain only port WWN members.

The **Add Member** button becomes active.

8. Click **Add Member** to add the zone member.

The selected member is moved to the Zone Members window.

9. *Optional:* Repeat steps 7 and 8 to add more elements to your zone.

10. *Optional:* Click **Add Other** to include a WWN or port that is not currently a part of the fabric.

At this point you can either save your changes or save and enable your changes.

11. Click **Zoning Actions**> **Save Config Only** to save the configuration changes.

To enable the configuration, see [“Enabling zone configurations”](#) on page 109.

ADDING AND REMOVING MEMBERS OF A ZONE

Use the following procedure to add or remove zone members.

To modify the members of a zone

1. Open the Zone Administration window as described on [page 96](#).
2. Click the **Zone** tab.
3. Select the zone you want to modify from the Name drop-down list.
The zone members for the selected zone are listed in the Zone Members list.
4. Highlight an element in the Member Selection List that you want to include in your zone, or highlight an element in the Zone Members list that you want to delete.
5. Click **Add Member** to add a zone member, or click **Remove Member** to remove a zone member.

The zone is modified in the Zone Admin buffer. At this point you can either save your changes or save and enable your changes.

6. Click **Zoning Actions**> **Save Config Only** to save the configuration changes.

To enable the configuration, see [“Enabling zone configurations”](#) on page 109.

RENAMING ZONES

Use the following procedure to change the name of a zone.

To rename a zone

1. Open the Zone Administration window as described on [page 96](#).
2. Click the **Zone** tab.
3. Select the zone you want to rename from the Name drop-down list.
4. Click **Rename**.
5. On Rename a Zone, type a new zone name and click **OK**.

The zone is renamed in the Zone Admin buffer. At this point you can either save your changes or save and enable your changes.

6. Click **Zoning Actions**> **Save Config Only** to save the configuration changes.

To enable the configuration, see [“Enabling zone configurations”](#) on page 109.

COPYING ZONES

Use the following procedure to copy a zone configuration.

To copy a zone

1. Open the Zone Administration window as described on [page 96](#).
2. Click the **Zone** tab.
3. Select the zone you want to delete from the Name drop-down list.
4. Click **Copy**.
5. On Copy an Existing Zone, enter a name for the copied zone.
6. Click **OK**.

The selected zone is copied from the Zone Admin buffer.

7. Click **Zoning Actions> Save Config Only** to save the configuration changes.

Since no changes were made to the effective configuration, you do not need to enable the configuration.

DELETING ZONES

Use the following procedure to delete a zone.

To delete a zone

1. Open the Zone Administration window as described on [page 96](#).
2. Click the **Zone** tab.
3. Select the zone you want to delete from the Name drop-down menu and click **Delete**.
4. On the confirmation dialog box, click **Yes**.

The selected zone is deleted from the Zone Admin buffer. At this point you can either save your changes or save and enable your changes.

5. Click **Zoning Actions> Save Config Only** to save the configuration changes.

To enable the configuration, see [“Enabling zone configurations”](#) on page 109.

Managing zone configurations

A zone configuration is a group of zones; zoning is enabled on a fabric by enabling a specific configuration. You can specify members of a configuration using zone names.

Figure 47 shows a sample zoning database and the relationship between the zone aliases, zones, and zoning configuration. The database contains one zoning configuration, *myconfig*, which contains two zones: *Zone A* and *Zone B*. The database also contains four aliases, which are members of *Zone A* and *Zone B*. *Zone A* and *Zone B* also have additional members other than the aliases.

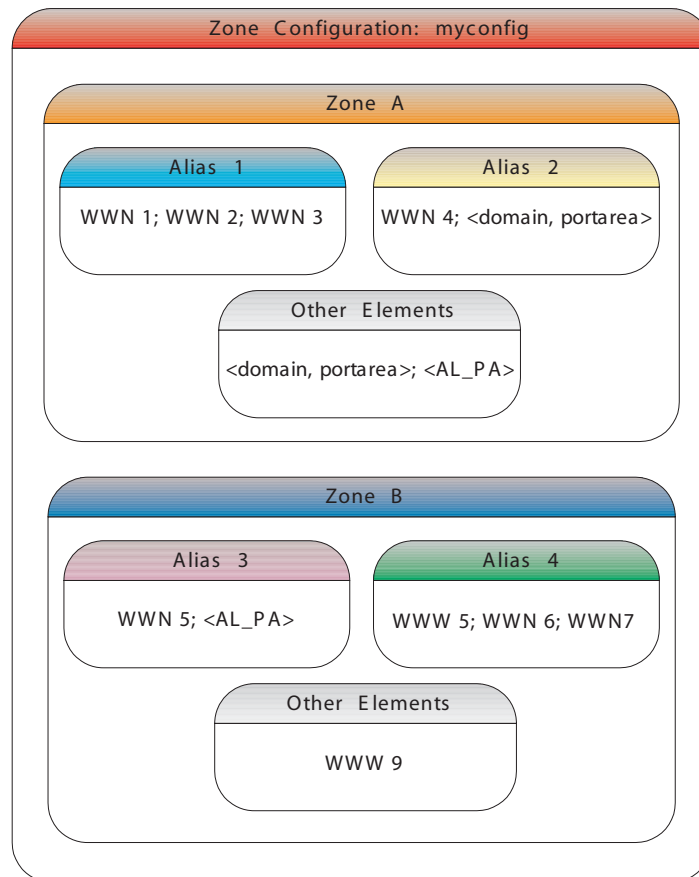


FIGURE 47 Sample zoning database

CREATING ZONE CONFIGURATIONS

Use the following procedure to create a zone configuration. After creating a zone configuration, you must explicitly enable it for it to take effect.

NOTE

Any changes made to the currently enabled configuration will not appear until you reenabling the configuration.

To create a zone configuration

1. Open the Zone Administration window as described on [page 96](#).
2. Select a format to display zoning members in the Member Selection List as described in "Zoning views" on page 101.
3. Click the **Zone Config** tab and click **New Zone Config**.

4. On **Create New Config**, type a name for the new configuration and click **OK**.
The new configuration appears in the Name drop-down list.
 5. Expand the **Member Selection List** to view the nested elements.
The choices available in the list depend on the selection made in the **View** menu.
 6. Select an element in the **Member Selection List** that you want to include in your configuration.
The **Add Member** button becomes active.
 7. Click **Add Member** to add configuration members.
Selected members are moved to the **Config Members Window**.
 8. Repeat steps 6 and 7 to add more elements to your configuration.
 9. Click **Zoning Actions > Save Config Only** to save the configuration changes.
- To enable the configuration, see [“Enabling zone configurations”](#) on page 109.

ADDING OR REMOVING ZONE CONFIGURATION MEMBERS

Use the following procedure to add or remove members of a zone configuration.

NOTE

You can make changes to a configuration that is currently enabled; however, changes will not appear until you reenable the configuration.

To modify the members of a zone configuration

1. Open the **Zone Administration** window as described on [page 96](#).
2. Click the **Zone Config** tab.
3. Select the configuration you want to modify from the Name drop-down list.
4. Click an element in the **Member Selection List** that you want to include in your configuration or click an element in the **Config Members** that you want to delete.
5. Click **Add Member** to add a configuration member or **Remove Member** to remove a configuration member.
6. Click **Zoning Actions > Save Config Only** to save the configuration changes.

To enable the configuration, see [“Enabling zone configurations”](#) on page 109.

RENAMING ZONE CONFIGURATIONS

Use the following procedure to change the name of a zone configuration.

NOTE

You cannot rename the currently enabled configuration.

To rename a zone configuration

1. Open the **Zone Administration** window as described on [page 96](#).
2. Click the **Zone Config** tab.

3. Select the configuration you want to rename from the Name drop-down list and click **Rename**.
4. On Rename a Config, type a new configuration name and click **OK**.
The configuration is renamed in the configuration database.
5. Click **Zoning Actions> Save Config Only** to save the configuration changes.

COPYING ZONE CONFIGURATIONS

Use the following procedure to copy a zone configuration.

To copy a zone

1. Open the Zone Administration window as described on [page 96](#).
2. Click the **Zone Config** tab.
3. Select the zone you want to delete from the Name drop-down list.
4. Click **Copy**.
5. On Copy An Existing Zone Config, enter a name for the copied zone and click **OK**.
The selected zone is copied from the Zone Admin buffer.
6. Click **Zoning Actions> Save Config Only** to save the configuration changes.

Since no changes were made to the effective configuration, you do not need to enable the configuration.

DELETING ZONE CONFIGURATIONS

Use the following procedure to delete a zone configuration.

NOTE

You cannot delete a currently enabled configuration.

To delete a disabled configuration

1. Open the Zone Administration window as described on [page 96](#).
2. Click the **Zone Config** tab.
3. Select the configuration you want to delete from the Name drop-down list and click **Delete**.
4. On the confirmation dialog box, click **Yes**.
The selected configuration is deleted from the configuration database.
5. Click **Zoning Actions> Save Config Only** to save the configuration changes.

ENABLING ZONE CONFIGURATIONS

Several zone configurations can reside on a switch at once, and you can quickly alternate between them. For example, you might want to have one configuration enabled during the business hours and another enabled overnight. However, only one zone configuration can be enabled at a time.

When you enable a zone configuration from Web Tools, the entire zoning database is automatically saved, and then the selected zone configuration is enabled.

If the zoning database size exceeds the maximum allowed, you cannot enable the zone configuration. The zoning database summary displays the maximum zoning database size (see [“Displaying zone configuration summaries”](#) on page 112).

To enable a zone configuration

1. Open the Zone Administration window as described on [page 96](#).
2. Click **Zoning Actions> Enable Config**.
3. On Enable Config, select the configuration to be enabled from the menu.
4. Click **OK** to save and enable the selected configuration.

DISABLING ZONE CONFIGURATIONS

When you disable the active configuration, the Advanced Zoning feature is disabled on the fabric, and all devices within the fabric can communicate with all other devices. This does not mean that the zoning database is deleted, however, only that there is no configuration active on the fabric.

When you disable a zone configuration from Web Tools, keep in mind that the entire zoning database is automatically saved, and then the selected zone configuration is disabled.

To disable a zone configuration

1. Open the Zone Administration window as described on [page 96](#).
2. Click **Zoning Actions> Disable Zoning**.
The Disable Config warning appears.
3. Click **Yes** to save and disable the current configuration.

DISPLAYING ENABLED ZONE CONFIGURATIONS

The enabled zone configuration screen displays the actual content of the single zone configuration that is currently enabled on the fabric, whether it matches the configuration that was enabled when the current Zone Administration session was launched or last refreshed (see [Figure 48](#) on page 111). The zones are displayed, and their contents (ports, WWNs) are displayed next to them. Aliases are not displayed in the enabled zone configuration. If there is no active zone configuration enabled on the switch, a message is displayed to that effect.

The enabled configuration is listed in the upper-right corner of the Zone Administration window.

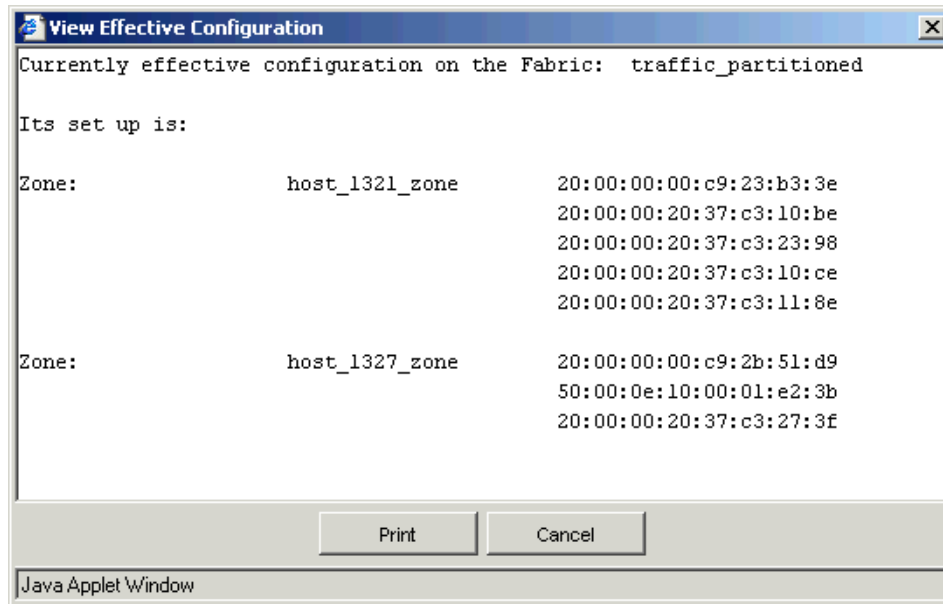


FIGURE 48 Effective Configuration window

To view the enabled zone configuration name without opening the Zone Administration window

1. Select a switch from the [Fabric Tree](#).

The selected switch appears in the [Switch View](#).

The current zone configuration name (if one is enabled) is displayed in the lower portion of the [Switch Events and Switch Information](#). If no zone configuration is enabled, the field displays “No configuration in effect”.

To view detailed information about the enabled zone configuration

1. Open the Zone Administration window, as described on [page 96](#).

The zone configuration in effect *at the time you launched the Zone Administration window* is identified in the upper-right corner. This information is automatically updated every 15 seconds. It is also updated if you manually refresh the Zone Administration window contents by clicking the refresh icon at the lower-right corner of the Zone Administration window, or when you enable a configuration through the Zone Administration window.

ATTENTION

Clicking the refresh icon overwrites all local unsaved zoning changes. If anyone has made any changes to the zones outside of your Zone Admin session, those changes will be applied.

2. To identify the most recently effective zone configuration *without* saving or applying any changes you have made in the Zone Administration window, click **File> Print Effective Zone Configuration** in the Zone Administration window.

If no zone is enabled, a message is displayed, indicating that there is no active zoning configuration on the switch.

3. *Optional:* Click **Print** located in the **Print Effective Zone Configuration** dialog box to print the enabled zone configuration details. This launches the print dialog box.

DISPLAYING ZONE CONFIGURATION SUMMARIES

The zone configuration summary hierarchically lists all defined zoning elements known to the current Zone Admin session, whether any of the listed configurations has been enabled, and whether any of the lower level elements has been added as members of the higher level (aliases, zones, FA zones) structures.

The zone configuration summary displays the entire contents of the fabric zoning database as it was at the time the Zone Admin session was launched, or the most recently saved or refreshed information, and any unsaved changes you make since the time the Zone Admin session is launched. It provides the name of the zone configuration that was enabled at the time you launched the Zone Admin session; however, keep in mind that the enabled configuration might have changed since then and that this screen will not reflect those changes.

To view a zone configuration summary report

1. Open the Zone Administration window as described on [page 96](#).
2. Click **File> Print Zone Database Summary**.

The Zone Configuration Summary window opens, as shown in [Figure 49](#).

The summary displays the information based on the changes just made. If current session changes have not yet been saved to the fabric, the information displayed here is different from what is seen from the switch.

3. *Optional:* Click **Print** to print the zone configuration summary.

This launches the print dialog box.

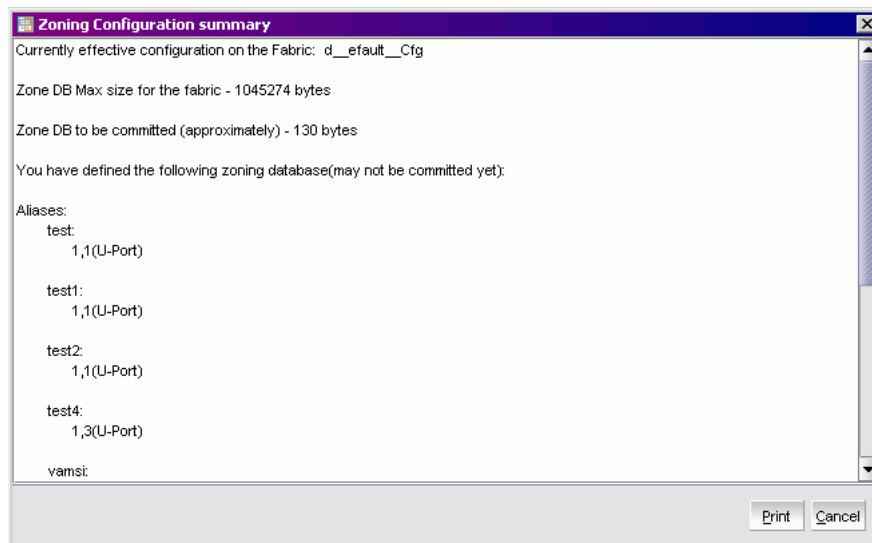


FIGURE 49 Zoning Configuration summary

CREATING CONFIGURATION ANALYSIS REPORTS

The configuration analysis report lists the following:

- SAN components that are not included in the configuration.
- SAN components that are in the configuration but not in the fabric.

To create a configuration analysis report

1. Open the Zone Administration window as described on [page 96](#).
2. Click the **Zone Config** tab.
3. Select a configuration to be analyzed from the Name drop-down list and click **Analyze Zone Config**.

A message opens to you if you want to refresh the fabric before running the analysis.

4. Click **Yes** or **No**.

The configuration analysis window displays.

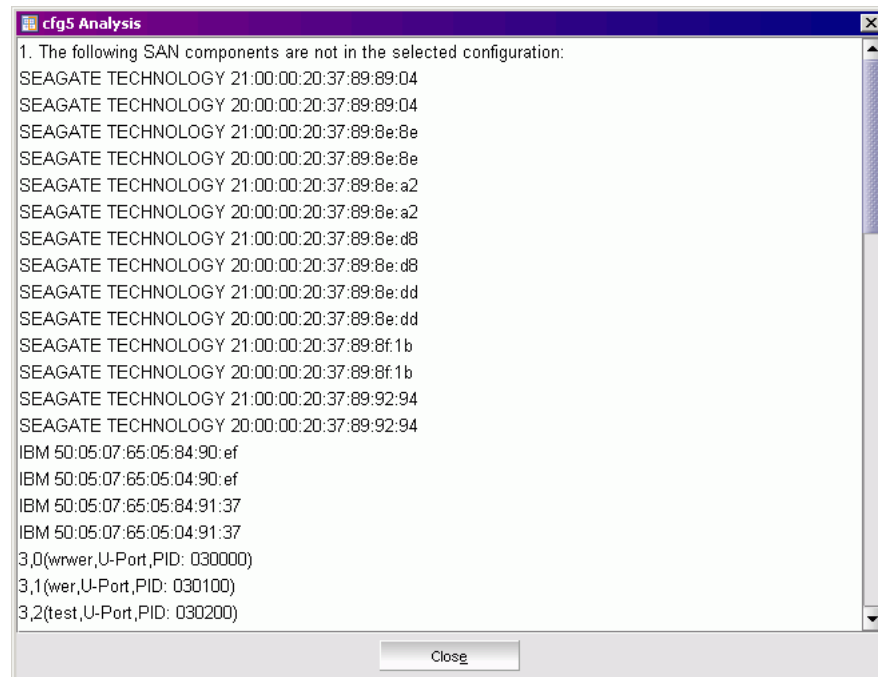


FIGURE 50 Configuration Analysis window

DISPLAYING ZONES INITIATOR/TARGET ACCESSIBILITY

The Initiator/Target Accessibility Matrix shows a list of initiators and a list of targets and indicates which initiator can access which target.

To display a Zones Initiator/Target Accessibility Matrix

1. Open the Zone Administration window as described on [page 96](#).
2. Click the **Zone Config** tab.
3. Select a configuration to be analyzed for device accessibility from the Name drop-down list.

4. Click **Device Accessibility**.

The Initiator/Target Accessibility Matrix for Config- Device Selection dialog box opens.

5. Select devices you want displayed in the accessibility matrix; click the radio button to select all devices in the fabric or to select a subset of the devices.

If you select a subset, you must click the devices from the Select Devices list and click **Add** to move them to the Evaluate for Accessibility list.

6. Click **OK**.

The Initiator/Target Accessibility Matrix displays. You can mouse over a target to display the symbolic name of the device. In addition, you can right-click the device nodes and click **View Device Detail** to display detailed information about the selected device.

Managing the zoning database

This section contains the following procedures for managing the zoning database:

- [“Adding a WWN to multiple aliases and zones,”](#) next
- [“Removing a WWN from multiple aliases and zones”](#) on page 115
- [“Replacing a WWN in Multiple Aliases and Zones”](#) on page 115
- [“Searching for zone members”](#) on page 115
- [“Clearing the Zoning Database”](#) on page 116
- [“Adding Unzoned Online Devices to a Zone or Alias”](#) on page 117
- [“Removing offline devices from the zoning database”](#) on page 118
- [“Replacing offline devices”](#) on page 118
- [“Defining device aliases”](#) on page 118

ADDING A WWN TO MULTIPLE ALIASES AND ZONES

This procedure enables you to configure a WWN as a member in a zone configuration prior to adding that device to the fabric. Specifically, it is useful if you want to add a WWN to all or most zoning entities. The added WWN does not need to currently exist in the fabric.

To add a WWN to the Zone Admin buffer

1. Open the Zone Administration window as described on [page 96](#).
2. Click **Edit> Add WWN**.

The Add WWN dialog box opens.

3. Type a WWN value in the WWN field and click **OK**.

The Add WWN dialog box displays all the zoning elements that will include the new WWNs. All of the elements are selected by default.

4. Click items in the list to select or unselect, and click **Add** to add the new WWN to all the selected zoning elements.

The WWN is added to the Zone Admin buffer and can be used as a member.

REMOVING A WWN FROM MULTIPLE ALIASES AND ZONES

Use this procedure if you want to remove a WWN from all or most zoning entities.

To delete a WWN from the Zone Admin buffer

1. Open the Zone Administration window as described on [page 96](#).
2. Click **Edit> Delete WWN**.
The Delete WWN dialog box opens.
3. Type a WWN value in the WWN field and click **OK**.
The Delete WWN dialog box displays all the zoning elements that include the WWN.
4. Click items in the list to select or unselect, and click **Delete** to delete the WWN from all the selected zoning elements.
The WWN is deleted from the selected items in the Zone Admin buffer.

REPLACING A WWN IN MULTIPLE ALIASES AND ZONES

This procedure enables you to replace a WWN throughout the Zone Admin buffer. This is helpful when exchanging devices in your fabric and helps you to maintain your current configuration.

To replace a WWN in the Zone Admin buffer

1. Launch the Zone Administration window as described on [page 96](#).
2. Click **Edit> Replace WWN**.
The Replace WWN dialog box opens.
3. Type the WWN to be replaced in the **Replace** field.
4. Type the new WWN in the **By** field and click **OK**.
The Replace WWN dialog box is displayed. It lists all the zoning elements that include the WWN.
5. Click an item in the list to select or unselect, and click **Replace** to replace the WWN in all the selected zoning elements.
The former WWN is replaced in the Zone Admin buffer by the new WWN, including within any alias or zone in which the old WWN was a member.

SEARCHING FOR ZONE MEMBERS

You can search zone member selection lists for specified strings of text. If you know some identifying information about a possible member of a zoning entity, you can select the tab and view for that entity and then search through its member selection list using the Search for Zone Member option. If the target entity is an alias or zone, then the search domain includes elements like switch names and domain numbers, port names and “domain, port” addresses, device WWNs and manufacturer names, and also any aliases that might already have been defined. If the target entity is a configuration, then zones are also included, along with the elements they contain.

The search starts from the top of the list, and when the target element is found, it is also selected in the Member Selection List so it can be added or its parent or children can be found. By default, the Member Selection List is searched from beginning to end one time. If you select the wraparound option, the search will continue to loop from the beginning to the end of the Member Selection List.

To search for a zone member

1. Open the Zone Administration window as described on [page 96](#).
2. Click **Edit> Search Member**.
3. Type the zone member name in the **Member Name** field.
Optional: Narrow the search by selecting one or more of the check boxes, such as **Match Case**.
4. Click **Next** to begin the zone member search.

CLEARING THE ZONING DATABASE

Use the following procedure to disable the active zoning configuration, if one exists, and delete the entire zoning database.

ATTENTION

This action not only disables zoning on the fabric but also deletes the entire zoning database. This results in all devices being able to communicate with each other.

To disable any active configuration and delete the entire zoning database

1. Open the Zone Administration window as described on [page 96](#).
2. Click **Actions> Clear All**.
The Disable Config warning opens.
3. Click **Yes** to do *all* of the following:
 - Disable the current configuration.
 - Clear the entire contents of the current Web Tools Zone Admin buffer.
 - Delete the entire persistent contents of the fabric zoning database.

CAUTION: This action is *not* recoverable.

USING ZONING WIZARDS

The Zone Administration window contains the following wizards to help you perform the following zoning tasks:

- Add unzoned devices
- Remove offline devices
- Replace offline devices
- Define device alias

Access the wizards through the Tools menu in the Zone Administration window. The following sections describe the zoning tasks and the procedure for accessing the wizards for each task. The wizards are self-explanatory, so the specific steps are not documented here.

NOTE

The left side of each wizard window lists the steps you need to take to complete the task. The current step is in blue, as shown in [Figure 51](#) on page 117. Some of the wizards allow you to loop and repeat the task multiple times; as a result, each step is listed in this panel, so that you not only see the steps that you still *need* to perform, but also the steps that you have *already* performed.

The step numbers do not necessarily match the overall numbering in this panel.

Adding Unzoned Online Devices to a Zone or Alias

When zoning is enabled, devices that are not included in a zone configuration are inaccessible to other devices in the fabric. Use the following procedure to identify online devices that are not zoned in any zone configuration and add them to a zone or alias.

To add unzoned online devices to a zone or alias

1. Open the Zone Administration window as described on [page 96](#).
2. Click **Tools> Add Unzoned Devices**.

The Add Unzoned Devices wizard opens.

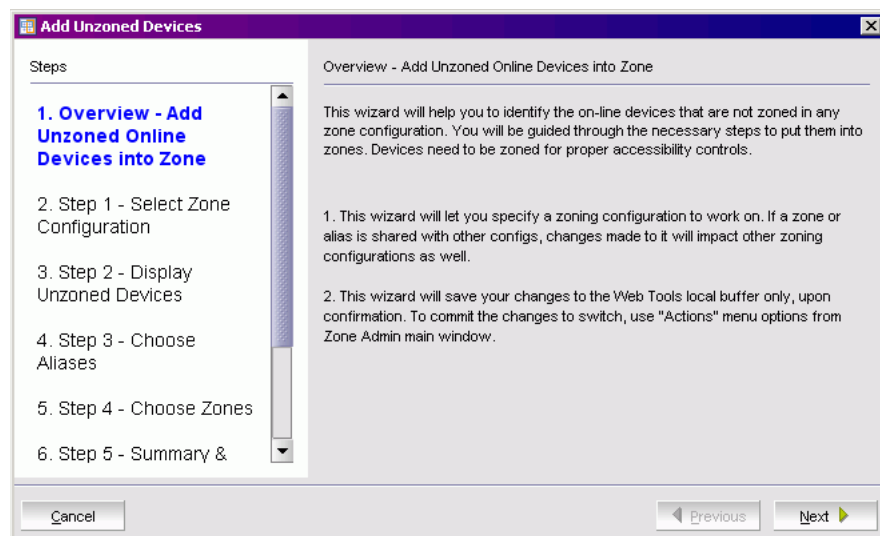


FIGURE 51 Add Unzoned Devices wizard

3. Follow the steps outlined in the wizard.

The wizard displays unzoned devices and prompts you to select them and add them to an alias or a zone.

When you have finished the steps for adding a device to a zone or alias, if there are any more unzoned devices, you can either continue to add those unzoned devices or exit the wizard. If there are no more unzoned devices, you must exit the wizard.

Removing offline devices from the zoning database

Removing offline devices (WWNs) helps clean the zoning database to save more space for new entries. Use the following procedure to view all devices that are no longer online and remove all or selected offline devices from the zoning database.

To remove offline devices from the zoning database

1. Open the Zone Administration window as described on [page 96](#).
2. Click **Tools> Remove Offline Devices**.

The Remove Offline Devices wizard opens.

3. Follow the steps outlined in the wizard.

The wizard allows you to view all devices that are no longer online, and remove all or selected offline devices from the zoning database.

Replacing offline devices

Replacing an offline device replaces its WWN with a new given WWN in all of its containing aliases and zones. Use the following procedure to view offline devices and replace them with new ones in the zoning database.

To replace offline devices

1. Open the Zone Administration window as described on [page 96](#).
2. Click **Tools> Replace Offline Devices**.

The Replace Offline Devices wizard opens.

3. Follow the steps outlined in the wizard.

The wizard allows you to view all devices that are no longer online, and replace all or selected offline devices with new ones (WWNs) in the zoning database.

Defining device aliases

Use the following procedure to define zone alias names for devices in a single process. This procedure is especially useful if you use one unique zone alias to name each device port.

The alias definitions of the devices are saved in the zoning database on the switch, which has a size limit. If database size becomes a concern, reconsider your use of alias definitions.

To assign aliases to devices

1. Open the Zone Administration window as described on [page 96](#).
2. Click **Tools> Remove Offline or Inaccessible Devices**.

The Remove Offline or Inaccessible Devices wizard opens.

3. Follow the steps outlined in the wizard.

The wizard allows you to define one and only one name for each device port (WWN). Devices with one or more aliases are considered already named and are not displayed.

NOTE

To enter a zone alias name, double-click the Zone Alias field for each device, and type the name.

After typing each alias name, you must press **Enter** or click another zone alias field, or the wizard does not accept the name.

Best practices for zoning

The following are recommendations for using zoning:

- Always zone using the highest Fabric OS-level switch.
Switches with lower Fabric OS versions do not have the capability to view all the functionality that a newer Fabric OS provides as functionality is backwards compatible but not forwards compatible.
- Zone using the core switch versus an edge switch.
- Zone using a director over a switch.
A director has more resources to handle zoning changes and implementations.
- Zone on the switch you connect to when bringing up Web Tools (the proxy switch).

Monitoring Performance

In this chapter

This chapter contains the following sections:

- [Monitoring performance using Web Tools 121](#)
- [Opening the Performance Monitoring window 126](#)
- [Creating basic performance monitor graphs 127](#)
- [Customizing basic monitoring graphs 127](#)
- [Creating advanced performance monitoring graphs 129](#)
- [Managing performance graphs 132](#)

Monitoring performance using Web Tools

The Web Tools Performance Monitoring window graphically displays throughput (in megabytes per second) for each port and for the entire switch.

The basic-mode Performance Monitor is standard in the Web Tools software. Any user logged into Web tools with an associated role of zoneadmin or securityadmin cannot open performance monitor. The roles user, operator, and basicswitchadmin are allowed to perform basic-mode performance monitor tasks except save or display canvas operations in any Admin Domain context. Only users with the admin, switchadmin and fabricadmin roles associated with their login accounts are able to save or display a canvas.

The Advanced Monitoring menu in performance monitor is an optionally licensed software. To utilize the Advanced Monitoring feature you must have a license installed and you must log in using an account that has an admin, switchadmin, or fabricadmin role.

Use the basic-mode Performance Monitoring window to:

- Create user-definable reports.
- Display a performance canvas for application-level or fabric-level views.
- Save persistent graphs across reboots (saves parameter data across reboots).

Using Brocade Advanced Performance Monitoring, you can display predefined reports for AL_PA, end-to-end, and filter-based performance monitoring. You can track:

- The number of CRC errors for AL_PA devices.
- The number of words received and transmitted in Fibre Channel frames with a defined S_ID/D_ID pair.
- The number of times a particular filter pattern in a frame is transmitted by a port.

For detailed information on performance monitoring, see the *Fabric OS Administrator's Guide*.

Each graph is displayed individually in a window, so it can be minimized, maximized, resized, and closed.

Graphs within the Performance Monitoring window are updated every 30 seconds. When you first display the graph or if you modify the graph (such as to add additional ports), you might have to wait up to 30 seconds before the new values are shown.

When you have multiple graphs open in the Performance Monitoring window, you can:

- Click **Window> Tile** to view all graphs at once, tiled in the Performance Monitoring window.
- Select **Window> Cascade** to view one graph at a time.
- Select **Window> Close All** to close all open Performance Monitor graphs in the Performance Monitoring window.

In addition, the Window menu lists all open graphs. You can click **Window**, and then select a graph name to view that graph.

Admin Domain considerations:

- If you are not the switch owner, you will see the following ports:
 - E_ports, including EX_Ports
 - directly owned ports
 - indirect ports
- You can use the Advanced Performance Monitoring feature only in AD255 or in AD0 if there are no other user-defined Admin Domains. Otherwise, access to Advanced Monitoring features in the Performance Graphs menu will be unavailable.
- It is recommended that you define a user with a switchadmin role and give that user access to AD255 for the purpose of data collecting using the Advanced Performance Monitor.

PREDEFINED PERFORMANCE GRAPHS

Web Tools predefines basic graph types, to simplify performance monitoring. A wide range of end-to-end fabric, LUN, device, and port metrics graphs are included.

[Table 6](#) lists the basic monitoring graphs available. [Table 7](#) on page 123 lists the advanced monitoring graphs.

The advanced monitoring graphs give more detailed performance information to help you manage your fabric. You can access the basic monitoring graphs on all switches; advanced monitoring graphs are available only on switches that have a Brocade Advanced Performance Monitoring license activated.

TABLE 6 Basic performance graphs

Graph Type	Displays
Port Throughput	The performance of a port, in bytes per second, for frames received and transmitted.
Switch Aggregate Throughput	The aggregate performance of all ports on a switch.
Blade Aggregate Throughput	The aggregate performance of all ports on a port card. This graph is available only for the Brocade 24000 and 48000 directors.
Switch Throughput Utilization	The port throughput, in Gbit/sec, at the time the sample is taken. For the Brocade 24000 and 48000 directors, this graph displays the throughput for each slot. You can customize this graph to display information for particular ports.
Port Error	CRC errors for a given port.
Switch Percent Utilization	The percentage utilization for each port in a switch. For the Brocade 24000 and 48000 directors, this graph displays the percent utilization for each slot. You can customize this graph to display information for particular ports.
Port Snapshot Error	The CRC error count between sampling periods for all the ports on a switch. For the Brocade 24000 and 48000 directors, this graph displays the CRC error rate for each slot. You can customize this graph to display information for particular ports.

TABLE 7 Advanced performance monitoring graphs

Graph Type	Displays
SID/DID Performance	The traffic between the SID-DID pair on the switch being managed. For more information, see “Creating SID-DID Performance Graphs” on page 129.
SCSI vs. IP Traffic	The percentage of SCSI versus IP frame traffic on each individual port. For more information, see “Creating an SCSI vs. IP Traffic Graph” on page 130.
AL_PA Errors	CRC errors for a given port and a given AL_PA. For more information, see “Creating AL_PA Error Graphs” on page 132.
SCSI Commands by port and LUN (R, W, R/W)	The total number of read/write commands on a given port to a specific LUN. For more information, see “Creating SCSI Command Graphs” on page 131.

The Brocade 48000 with an FC4-18i and the Brocade 7500 include physical FC ports, logical FC ports, and GbE ports. The Brocade 48000 with a or FC4-16IP blade includes physical FC ports and GbE ports. Not all of the performance monitoring graphs support the logical FC ports and GbE ports.

Table 8 lists each graph and indicates the supported port types for each. The port selection lists for each graph display the supported ports for that graph.

TABLE 8 Supported port types for Brocade 7500 and 48000

Graph Type	Physical FC_Ports	Logical FC_Ports	GbE Ports
Port Throughput	P	P	P
Switch Aggregate Throughput	N/A	N/A	N/A
Blade Aggregate Throughput ¹	N/A	N/A	N/A
Switch Throughput Utilization	P		P
Port Error	P	P	P
Switch Percent Utilization	P		P
Port Snapshot Error	P	P	
SID/DID Performance	P	P	
SCSI Commands	P		
SCSI vs. IP Traffic	P		
ALPA Error ²	P		

1. Blade Aggregate Throughput graph is not supported on the Brocade 7500 switch.

2. ALPA Error graph is not supported on the Brocade 7500, Brocade 7600, or on the Brocade 48000 director with an FC4-18i, FC4-16IP, or FC4-18, FC4-48 blade.

The labeling of axes in the graphs depends on the switch type.

- For the Brocade 24000 and 48000 directors, slot numbers are displayed with expansion arrows next to them, as shown in Figure 52 on page 125. Click the arrows to expand and contract the list of ports per slot.
- For the Brocade 200E, 3250, 3850, 3900, 4012, 4016, 4018, 4020, 4024, 4100, 4900, 5000, and 7500 switches, slot numbers are not identified.

For the Switch Throughput Utilization graph, the X-axis depends on the switch type.

- For Brocade 24000 and 48000 directors, the X-axis scales up to 102.4 Gbit/sec in multiples of 2.
- For Brocade 200E, 3250, 3850, 3900, 4012, 4016, 4018, 4020, 4024, 4100, 4900, 5000, 7500, and 7600 switches, the X-axis scales up to 4.0 Gbit/sec in increments of 0.4 Gbps.

Port throughput utilization is represented by a horizontal bar for each selected port, which gets longer or shorter depending on the percent utilization for that port at the last poll time. Thin short vertical intersecting bars give a historical perspective by representing the highest and lowest values reached for each selected port since the graph was opened. A third bar between them represents the average of all values polled (see Figure 52).

Figure 52 shows how to access the list of Advanced Performance Monitoring graphs using Web Tools. This example displays the graphs available in the Performance Monitoring window for a Brocade 24000 director with the Advanced Performance Monitoring license installed. Note that the slot number is identified.

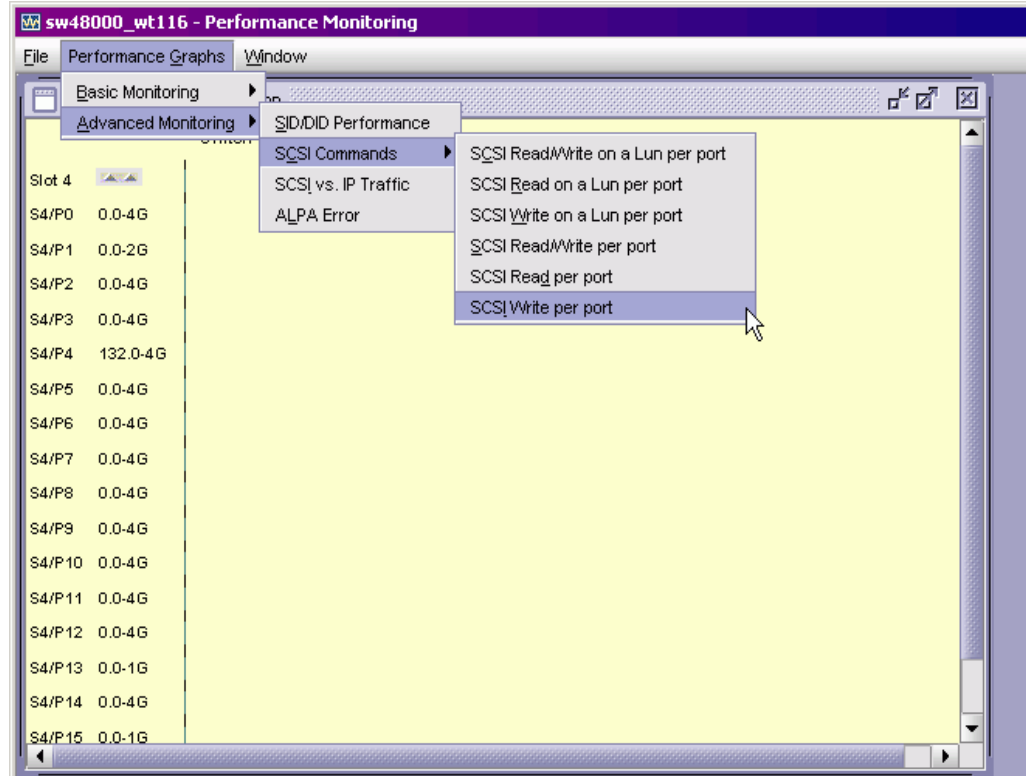


FIGURE 52 Accessing performance graphs

USER-DEFINED GRAPHS

You can modify the predefined graphs to create your own customized graphs (see [“Customizing basic monitoring graphs”](#) on page 127 for more information). These user-defined graphs can be added and saved to canvas configurations, described next.

CANVAS CONFIGURATIONS

A “canvas” is a saved configuration of graphs. The graphs can be either the Web Tools predefined graphs or user-defined graphs. Each canvas can hold up to eight graphs per window, with six shown in [Figure 53](#). Up to 20 canvases can be set up for different users or different scenarios. Each canvas is saved with a name and an optional brief description.

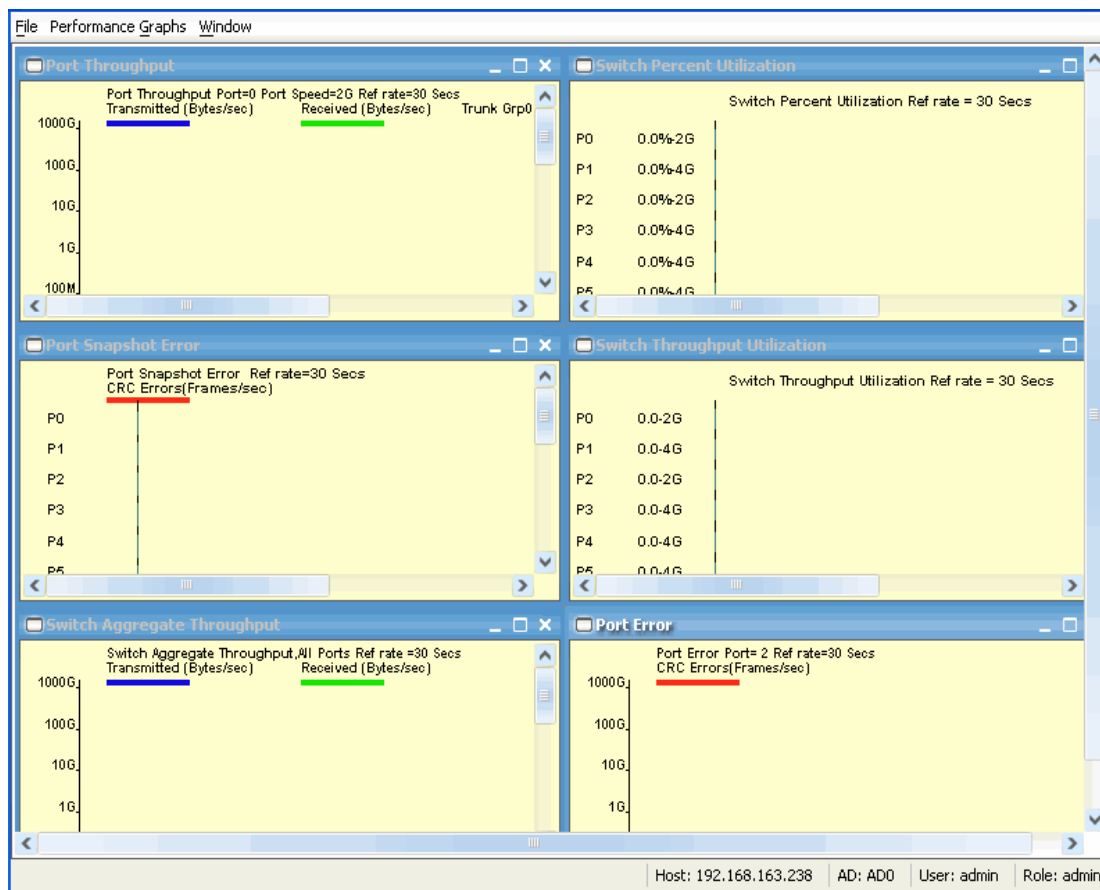


FIGURE 53 Canvas of six performance monitoring graphs

Opening the Performance Monitoring window

Use the following procedure to open the Web Tools Performance Monitoring window.

To open the Performance Monitoring window

1. Select a switch from the Fabric Tree and log in when prompted.
2. In the Monitor area under Tasks, click **Performance Monitor**.

The **Performance Monitoring** window opens.

Creating basic performance monitor graphs

Use the following procedure to create the basic performance monitor graphs listed in [Table 6](#) on page 123.

To create a basic performance monitor graph

1. Open the Performance Monitor window.
2. Click **Performance Graphs> Basic Monitoring> Graph Type**.

Depending on the type of graph you select, you might be prompted to select a slot or port for which to create a graph (see [Figure 55](#)).

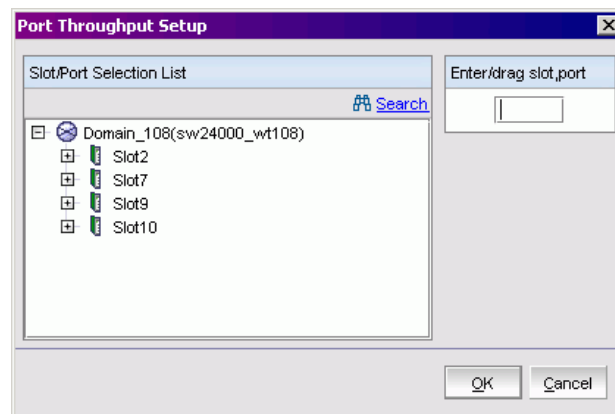


FIGURE 54 Creating a basic performance monitor graph

3. If prompted, drag the port into the **Enter/drag slot,port** field, or manually type the slot and port information in the field, in the format *slot,port*.

For Brocade 200E, 3250, 3850, 3900, 4012, 4016, 4018, 4020, 4024, 4100, 4900, 5000, 7500, and 7600 switches enter only a port number.

4. Click **OK**.

The graph is displayed in a window in the Performance Monitoring window. The following section explains how you can customize some of these graphs.

Customizing basic monitoring graphs

You can customize some of the basic performance monitoring graphs to display information for particular ports. For the Brocade 24000 and 48000 directors, you can also customize these graphs to display information for a slot.

You can customize the following graphs:

- Switch Throughput Utilization
- Switch Percent Utilization
- Port Snapshot Error

The following procedure assumes that you have already created one of these customizable graphs.

To customize basic performance monitoring graphs

1. Create or access the graph you want to customize. See [“Creating basic performance monitor graphs”](#) on page 127 for instructions on creating a graph.
2. **For Brocade 24000 and 48000 directors**, to display detailed port throughput utilization rates for each port in a slot, click the arrows next to a slot. Port information for that slot is displayed in the graph.

For Brocade 200E, 3250, 3850, 3900, 4012, 4016, 4018, 4020, 4024, 4100, 4900, 5000, 7500, and 7600 switches, proceed to [step 3](#).

3. To display detailed port throughput utilization rates for particular ports only, right-click anywhere in the graph and click **Select Ports**.

The setup dialog box displays, as shown in [Figure 55](#). The title of the dialog box varies, depending on the type of graph you are customizing, but the layout of the dialog box is the same. [Figure 55](#) shows an example of the setup dialog box for the Switch Throughput Utilization graph.

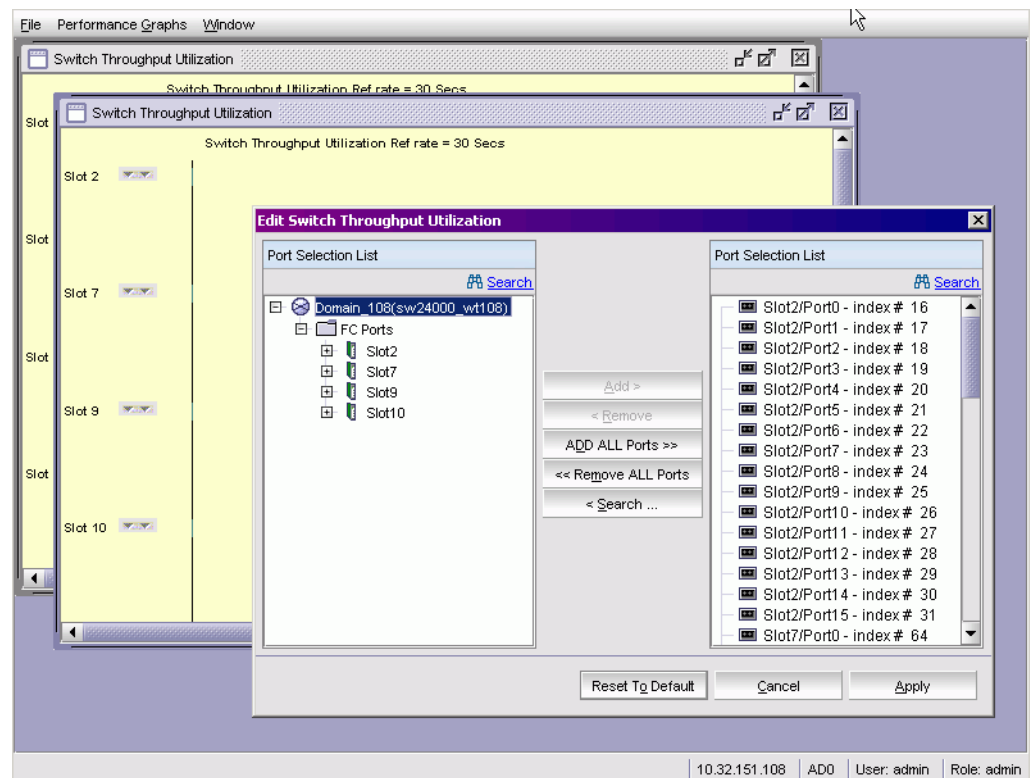


FIGURE 55 Select Ports dialog box for customizing Switch Throughput Utilization graph

You can perform the following in the dialog box:

- a. Double-click the domain to expand the slot/port list.

For the Brocade 24000 and 48000 directors, click the + signs to expand the ports under each slot, as shown in [Figure 55](#).

- b. Click the port you want to monitor in the graph in the Port Selection List. Use Shift-click and Ctrl-click to select multiple ports.

- c. Click **Add** to move the selected ports to the Selected Ports list.
- d. *Optional:* Click **ADD ALL Ports** to add all of the ports in the Port Selection List to the Selected Ports list.
- e. *Optional:* Click **Search** to open the Search Port Selection List dialog box, from which you can search for all E_Ports, all F_Ports, or all port names with a defined string. Select the ports you want to add and click **Search** in the Search Port Selection List dialog box.
- f. Click **Apply**.

Only the selected ports are displayed in the graph.

Creating advanced performance monitoring graphs

This section describes how to create the advanced performance monitor graphs listed in [Table 7](#) on page 123. Because the procedure for creating these graphs differs depending on the type of graph, each type is described separately in the sections that follow.

The advanced monitoring graphs are not supported for GbE ports.

NOTE

You must have an Advanced Performance Monitoring license installed to use the Advance Performance Monitor features. If user-defined Admin Domains have been configured, Advanced Performance Monitoring works only in AD255.

CREATING SID-DID PERFORMANCE GRAPHS

The SID/DID Performance graph displays the traffic between a SID-DID pair on the switch being managed.

To create an SID/DID performance graph

1. Open the Performance Monitoring window.
2. Click **Performance Graphs> Advanced Monitoring> SID/DID Performance**.

The SID/DID Performance Setup dialog box displays (see [Figure 56](#) on page 130).

- To see which end-to-end (EE) monitors are currently set up on a particular port, proceed to [step 3](#).

9 Creating advanced performance monitoring graphs

- To specify the port, Source ID and Domain ID, skip to [step 4](#).

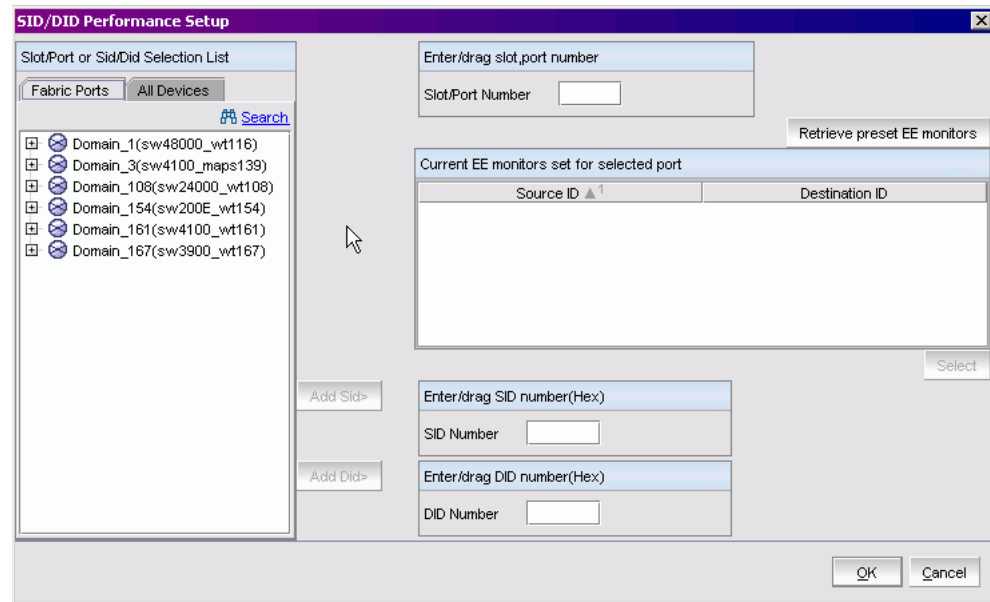


FIGURE 56 Creating an SID/DID performance graph

3. Click a port from the Slot/Port or Sid/Did Selection List.
 - a. Drag the selected port into the Enter/drag port number field.
 - b. Click **Retrieve preset EE monitors**.

The current end-to-end monitors for that port are displayed in the “Current EE monitors set for selected port” table.
 - c. *Optional:* To display a performance graph for the current EE monitors set for the selected port, click a SID-DID pair in the table. You can select multiple source ID and Destination IDs. Click **Select**. If you selected multiple SID/DID monitors, click **OK** in the confirmation dialog box that appears. Skip to [step 6](#).

If you do not want to display a performance graph for the current EE monitors set for the selected port, continue with [step 4](#).
4. Click a source ID from the “Port or Sid/Did Selection List,” and click **Add Sid**. You can also type a source ID in the “Enter/drag SID number” field.
5. Click a destination ID from the “Port or Sid/Did Selection List,” and click **Add Did**. You can also type a destination ID in the “Enter/drag DID number” field.
6. Click **OK**.

If you selected multiple EE monitors, SIDs, or PIDs, a confirmation dialog box displays, reminding you that one graph will be opened for each selection. Click **Yes** to display the graphs.

CREATING AN SCSI VS. IP TRAFFIC GRAPH

The SCSI vs. IP Traffic graph displays the SCSI versus IP traffic for selected ports. For Brocade 24000 and 48000 directors, the slot and port name is identified in the graph.

In a trunk group, the SCSI vs. IP Traffic graph displays only the master port and not the slave ports.

To create a SCSI vs. IP Traffic graph

1. Open the Performance Monitoring window.
2. Click **Performance Graphs> Advanced Monitoring> SCSI vs. IP Traffic**.
The SCSI vs. IP Traffic Setup dialog box opens. This dialog box is similar to that shown in [Figure 55](#) on page 128.
3. Double-click the domain to expand the slot/port list.
For Brocade 24000 and 48000 directors, click the + signs to expand the ports under each slot, as shown in [Figure 55](#).
4. Click the port you want to monitor in the graph in the Port Selection List. Use Shift-click and Ctrl-click to select multiple ports.
5. Click **Add** to move the selected ports to the Selected Ports list.
6. *Optional:* Click **ADD ALL Ports** to add all of the ports in the Port Selection List to the Selected Ports list.
7. *Optional:* Click **Search** to open the Search Port Selection List dialog box, from which you can search for all E_Ports, all F_Ports, or all port names with a defined string. Select the ports you want to add and click **Search** in the Search Port Selection List dialog box.
8. Click **Apply** in the SCSI vs. IP Traffic Setup dialog box.
Only the selected ports are displayed in the SCSI vs. IP traffic graph.

CREATING SCSI COMMAND GRAPHS

This graph displays the total number of read or write (or both) commands on a given port or to a specific LUN on a given port.

To create a SCSI command graph

1. Open the Performance Monitoring window.
2. Click **Performance Graphs> Advanced Monitoring> SCSI Commands> Graph Type**.
The applicable setup dialog box displays. [Figure 57](#) on page 131 shows the “SCSI Read/Write on a LUN per port Setup” dialog box.

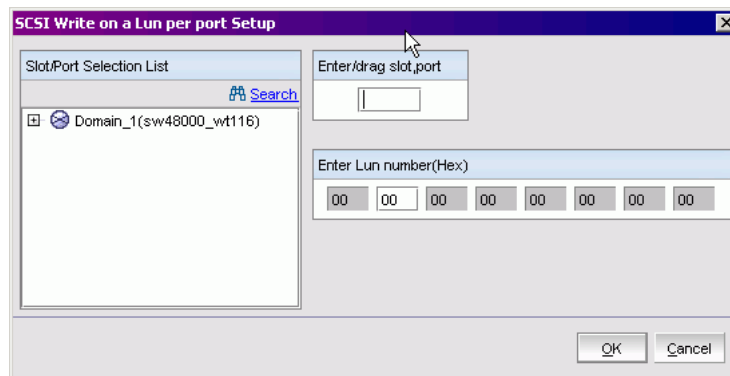


FIGURE 57 Creating a SCSI command graph

3. Navigate to a switch> slot> port in the Slot/Port Selection List.

- Click the port from the Slot/Port Selection List and drag it into the Enter/drag slot,port field.
- Optional:* For the LUN per port graphs, type a LUN number, in hexadecimal notation.

For the Brocade 4100 or 5000 switch, you can enter up to eight LUN masks.
For the Brocade 48000 director, you can enter up to four LUN masks.
For all other switches running Fabric OS 4.x or v5.x, you can enter up to two LUN masks.
For switches running Fabric OS 3.x, you can enter up to three LUN masks.
- Click **OK**.

The selected graph is displayed in the canvas.

CREATING AL_PA ERROR GRAPHS

The AL_PA Error graph displays CRC errors for a given port and a given AL_PA. The AL_PA Error graph is not supported on the following:

- Brocade 200E, 4012, 4016, 4018, 4020, 4024, 4100, 4900, 5000, 7500, and 7600
- Brocade 48000 with an FR4-18i, FC4-16IP, FC-18 or FC4-48 blade(s) installed

To create an AL_PA error graph

- Open the Performance Monitoring window.
- Click **Performance Graphs> Advanced Monitoring> ALPA Error**.

The ALPA Error Setup dialog box opens.
- Navigate to a switch> slot> port in the Slot/Port or Alpa Selection List.
- Click the port from the Slot/Port Selection List or an AL_PA from the Slot/Port Selection List, and drag it into the “Enter/drag slot,port” field. You can also manually type the slot and port number, in the format *slot,port*.
- Click **OK**.

The AL_PA Error graph opens on the canvas.

Managing performance graphs

This section provides the following procedures for managing performance graphs:

- [Saving graphs to a canvas](#) 132
- [Adding graphs to a canvas](#) 133
- [Printing graphs](#) 133
- [Modifying graphs](#) 134

SAVING GRAPHS TO A CANVAS

Saving graphs is especially useful when you create customized graphs and do not want to re-create them every time you access the Performance Monitoring window.

When you save graphs, you must save them to a canvas. The following procedure describes how to save graphs to a new canvas.

To save graphs

1. Open the Performance Monitoring window.
2. Create basic or advanced Performance Monitor graphs, as described in [“Creating basic performance monitor graphs”](#) on page 127 and [“Creating advanced performance monitoring graphs”](#) on page 129.

The graphs are displayed in the Performance Monitor window.

3. Click **File> Save Current Canvas Configuration**.

The Save Canvas Configuration dialog box opens.

4. Type a name and description for the configuration and click **Save Canvas**.

A message displays, confirming that the configuration was successfully saved to the switch.

ADDING GRAPHS TO A CANVAS

The following procedure assumes that a canvas is already created.

To create a new canvas, you must first create graphs, as described in [“Creating basic performance monitor graphs”](#) on page 127 and [“Creating advanced performance monitoring graphs”](#) on page 129, and then save those graphs to a canvas, as described in [“Saving graphs to a canvas”](#) on page 132.

To add a graph to an existing canvas

1. Click **File> Display Canvas Configurations**.

The Canvas Configuration List displays. A message “No Canvas configuration to display” will display if there are no saved canvas configurations.

2. Click a canvas in the list.
3. Click **Edit**.

The Edit Canvas dialog box displays.

4. Click **Add**.

A list of graphs displays.

5. Click a graph to add it to the canvas, and click **Save**.

PRINTING GRAPHS

You can print a single graph or all the graphs displayed on the selected canvas configuration. Only one canvas configuration can be opened at a time.

To print a single graph

1. Open the Performance Monitoring window.
2. Create a basic or advanced Performance Monitor graph as described in [“Creating basic performance monitor graphs”](#) on page 127 and [“Creating advanced performance monitoring graphs”](#) on page 129.
3. Right-click the graph and choose **Print**.
4. In the print dialog box, click **OK**.

To print all graphs in a canvas

1. Open the Performance Monitoring window.
2. Click **File> Print All Graphs**.
3. In the print dialog box, click **OK**.

MODIFYING GRAPHS

Use the following procedure to modify an existing graph that is saved in a canvas.

To modify an existing graph

1. Open the Performance Monitoring window.
2. Click **File> Display Canvas Configurations**.

The Canvas Configuration List displays. A message “No Canvas configuration to display” displays if there are no saved canvas configurations.

3. Select a canvas from the list and click **Edit**.

The **Performance Monitor Canvas: Canvas Name** dialog box displays.

4. Select a graph from the list and click **Edit**.

NOTE

The **Edit** button is enabled only for the graphs that are configurable or editable.

5. Make changes in the Edit dialog box, as necessary.
6. Click **OK** to close the Edit dialog box.
7. Click **Save** to save the changes and close the Performance Monitor Canvas dialog box.
8. Click **Close** to close the Canvas Configuration List.

Using the FC-FC Routing Service

In this chapter

This chapter describes how to use the FC-FC Routing Service to share devices between fabrics without merging the fabrics. It contains the following information:

- [“Supported switches for fibre channel routing,”](#) next
- [“About fibre channel routing”](#) on page 135
- [“Setting up FC-FC routing”](#) on page 137
- [“Managing FC-FC routing with Web Tools”](#) on page 138
- [“Viewing and configuring EX_Ports”](#) on page 140
- [“Viewing and configuring LSAN zones”](#) on page 142
- [“Configuring the backbone fabric ID”](#) on page 144

Supported switches for fibre channel routing

The FC-FC Routing Service is supported only on the following switch models:

- Brocade 7500 switch
- Brocade 48000 director, when configured with an FR4-18i blade (see the *Fabric OS Administrator's Guide* for more information)
- Brocade AP7420

Any of the supported switches listed above are considered FC Router-capable. If an EX_Port is configured for that switch, the switch is FC-Router enabled.

See the *Web Tools—AP Edition Administrator's Guide* for information on setting up the FC-FC Routing Service on the Brocade AP7420.

About fibre channel routing

Fibre Channel routing provides connectivity to devices in different fabrics without merging the fabrics.

For example, using Fibre Channel routing you can share tape drives across multiple fabrics without the administrative problems, such as change management, network management, scalability, reliability, availability, and serviceability, that might result from merging the fabrics.

Fibre Channel routing allows you to create logical storage area networks (LSANs) that can span fabrics. These LSANs allow Fibre Channel zones to cross physical SAN boundaries without merging the fabrics and while maintaining the access controls of zones.

Descriptions of Fibre Channel routing includes some specific terminology:

backbone fabric	An FC Router can connect two edge fabrics; a <i>backbone fabric</i> connects FC Routers. The backbone fabric is the fabric to which the FC Router switch belongs. A backbone fabric consists of at least one FC Router and possibly a number of Fabric OS-based Fibre Channel switches. Initiators and targets in the edge fabric can communicate with devices in the backbone fabric through the FC Router.
edge fabric	A standard Fibre Channel fabric with targets and initiators connected through an FC Router to another Fibre Channel fabric.
EX_Port	A type of port that functions somewhat like an E_Port, but does not propagate fabric services or routing topology information from one fabric to another.
FC Router	A switch running FC-FC Routing Service.
interfabric link (IFL)	The link between an E_Port and an EX_Port, or a VE_Port and a VEX_Port.
metaSAN	The collection of all SANs interconnected with FC Routers.
VEX_Port	A virtual port that enables routing functionality via an FCIP tunnel. A VEX_Port is similar to an EX_Port.

NOTE

Devices on edge fabrics that are connected to a Brocade AP7420 Multiprotocol Router cannot communicate with devices in the backbone fabric.

[Figure 58](#) on page 137 shows a metaSAN with a backbone consisting of one FC Router connecting hosts in edge fabric 1 and 3 with storage in edge fabric 2 and the backbone fabric through the use of LSANs. A device is shared between:

- The backbone fabric and edge fabric 1
- Edge fabric 1 and edge fabric 2
- Edge fabric 2 and edge fabric 3

MCDATA INTEROPERABILITY

Brocade switches and McDATA legacy switches interoperate while operating in the open mode. With FCR, we can connect any Brocade to any McDATA fabric, without service disruption. All the existing features of the two fabrics remain the same, except that we are able to share devices between them.

NOTE

Web Tools does not work with McData edge-fabrics.

You can configure any EX_Port on a FCR to be either McDATA Open Mode or McDATA Fabric Mode. You can setup the LSANzone with the shared devices from both fabrics. Once these configurations are done, and the ports are connected, devices are shared just like connecting two Brocade fabrics.

FCR interoperates with McDATA edge fabrics in both the McDATA Open Mode 1.0 and the McDATA Fabric Mode. You have the ability to configure any EX_Port to connect to a McDATA fabric without disrupting the existing services. All the EX_Port functionality such as fabric isolation, device sharing, remains the same as connecting to an existing Brocade fabric.

When FCR is interoperating with McDATA edge fabrics in Fabric mode and Open mode, it will support the LSANzone with the backbone devices. FCR will support the following McDATA versions: v4.1.1, v5.x, v6.x, v7.x, v8.x. Since Brocade has no way of knowing how the modern McDATA switch will operate natively in the future, there is no guarantee that the 5.3.0 version of FCR will work with any future version of McDATA fabric.

NOTE

McDATA fabrics are supported only as edge fabrics and should not be tried in backbone fabrics.

For additional information about FC-FC routing, see the *Fabric OS Administrator's Guide*.

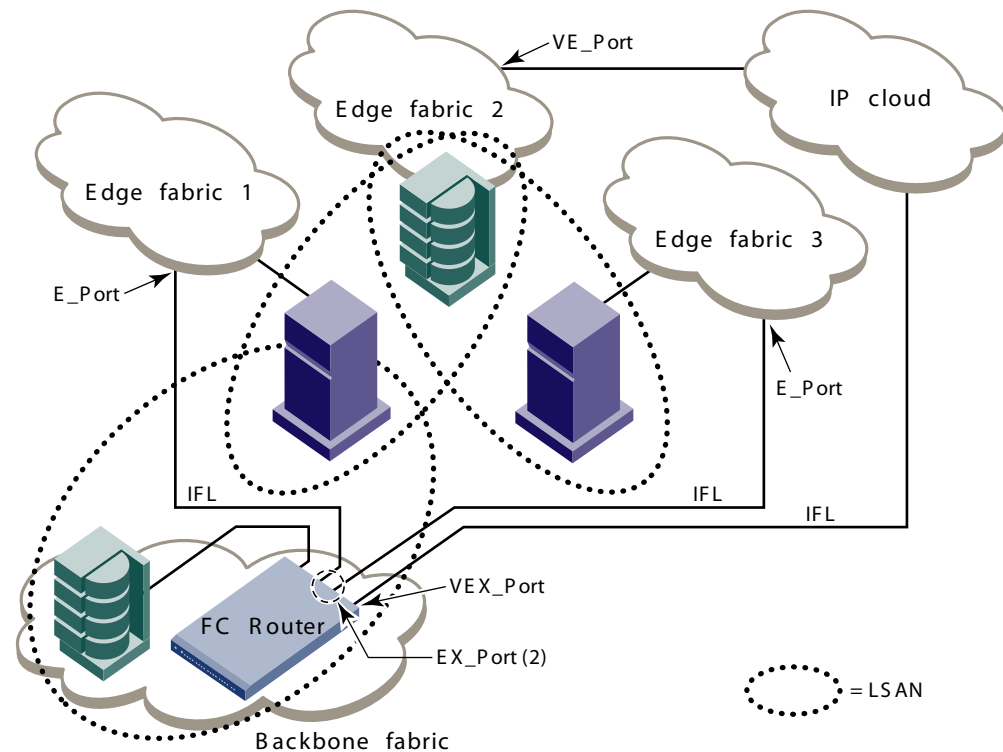


FIGURE 58 A metaSAN with edge-to-edge and backbone fabrics

Setting up FC-FC routing

The following procedure provides the basic steps for setting up FC-FC Routing using an FC Router.

1. Ensure that the backbone fabric ID of the FC Router is the same as that of other FC Routers in the backbone fabric. See [“Configuring the backbone fabric ID”](#) on page 144.
2. On the FC Router, ensure that the ports to be configured as EX_Ports are either not connected or are disabled.
3. Configure EX_Ports by clicking the **EX Ports** tab and then clicking **New**. Follow the instructions in the wizard. See [“Viewing and configuring EX_Ports”](#) on page 140.
4. Connect the cables from the EX_Ports on the FC Router to the edge fabrics, if they were not connected before.

For a multi-FC Router backbone fabric, make sure that each FC Router is connected to a switch in the backbone fabric.

5. Configure LSAN zones on the fabrics that will share devices. See [“Viewing and configuring LSAN zones”](#) on page 142.
6. View the information in the **EX Ports**, **LSAN Fabrics**, **LSAN Zones**, and **LSAN Devices** tabs to make sure that your configuration has succeeded.

Managing FC-FC routing with Web Tools

You manage FC-FC routing through the FC Routing module, shown in [Figure 59](#) on page 139. The FC Routing module has tabbed panes that display EX_Ports, LSAN fabrics, LSAN zones, LSAN devices, and general FCR information.

The FC Routing module provides a dynamic display. Any changes in the FCR configuration on the switch are automatically updated in the FC Routing module within 30 to 90 seconds, depending on the network traffic.

The switch must be FC Router-capable, as described in [“Supported switches for fibre channel routing”](#) on page 135.

The only things you need to configure on the FC Router are the EX_Ports and the backbone fabric ID. You configure LSAN zones on the fabrics from where devices need to be shared. You can configure LSAN zones on the backbone fabric to allow edge fabrics to share devices in the backbone fabric.

You must be logged in as admin or switchadmin to launch the FC Routing module. If you are logged in as a user role, you cannot access the FC Routing module.

If the FC-FC Routing service is disabled, the LSAN zones, LSAN fabric, and devices tabs will continue to show the existing entries but it will show the entries related to the *backbone fabric* only. All of the EX_Ports are disabled and you cannot enable them until FC-FC routing is enabled.

LAUNCHING THE FC ROUTING MODULE

The **FCR** button in the Switch View launches the FC Routing module. This button is displayed only for the following switches:

- Brocade 7500 switch
- Brocade 48000 director configured with an FR4-18i blade

To access the FC Routing module

1. Select a switch from the [Fabric Tree](#).

The selected switch appears in the [Switch View](#).

2. Click **FCR** in the **Manage** section of the **Tasks** menu.

The FC Routing module displays (as shown in Figure 59). If FC-FC Routing is disabled, a message to that effect displays on all the tabs in the module.

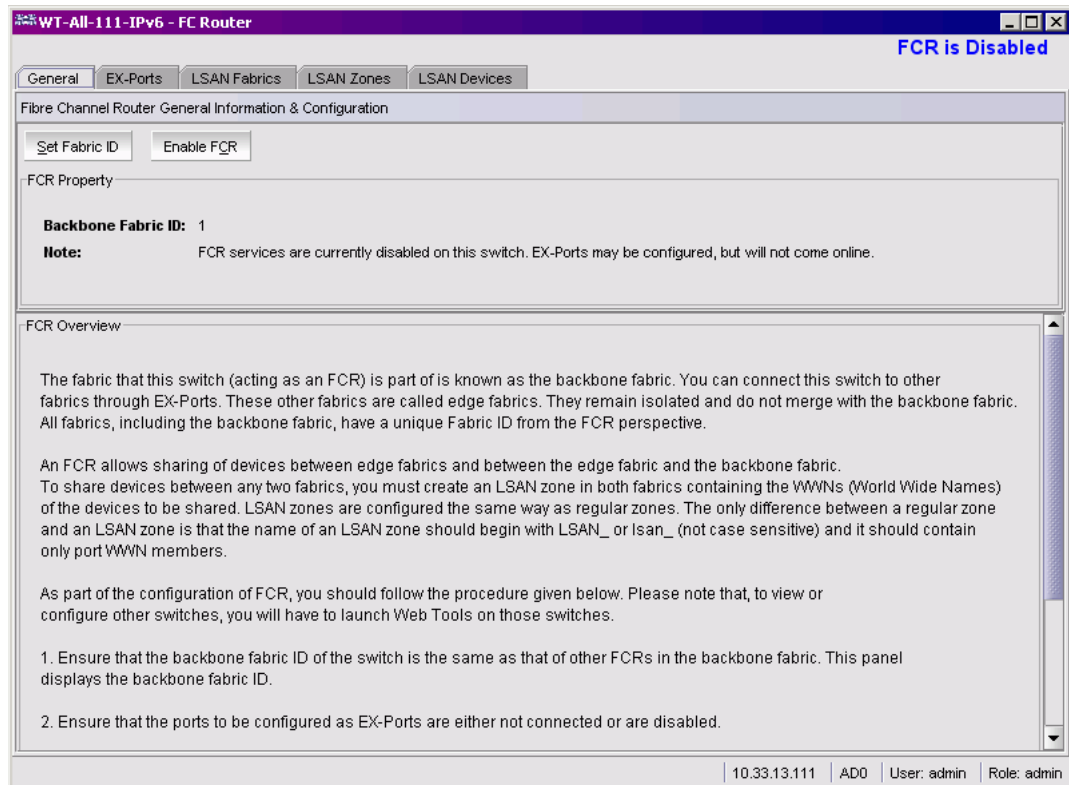


FIGURE 59 FC Routing module in Disabled mode with General tab selected

VIEWING AND MANAGING LSAN FABRICS

The **LSAN Fabric** tab (see Figure 60 on page 140) displays all the LSAN fabrics visible to your switch, in both a tabular and tree form. (If FC-FC Routing is disabled, the tables and tree nodes in this tab are empty.)

For more detailed information about a specific LSAN fabric, click a fabric name in the table and then click View Details in the task bar. You can also click the fabric name in the tree on the left side of the window.

When there is more than one router present in the backbone fabric with different backbone Fabric IDs, the routers with the conflicting IDs are shown in a separate table on the LSAN Fabric tab.

To manage an LSAN fabric, select the fabric to manage (either by clicking a row in the table or by clicking the fabric name in the tree) and click Manage LSAN Fabric in the task bar. A browser window is launched with the following url:

`http://ip-address-of-lsan-fabric-switch`

For Brocade switches, this launches Web Tools. For non-Brocade fabrics, this launches the element manager for that switch.

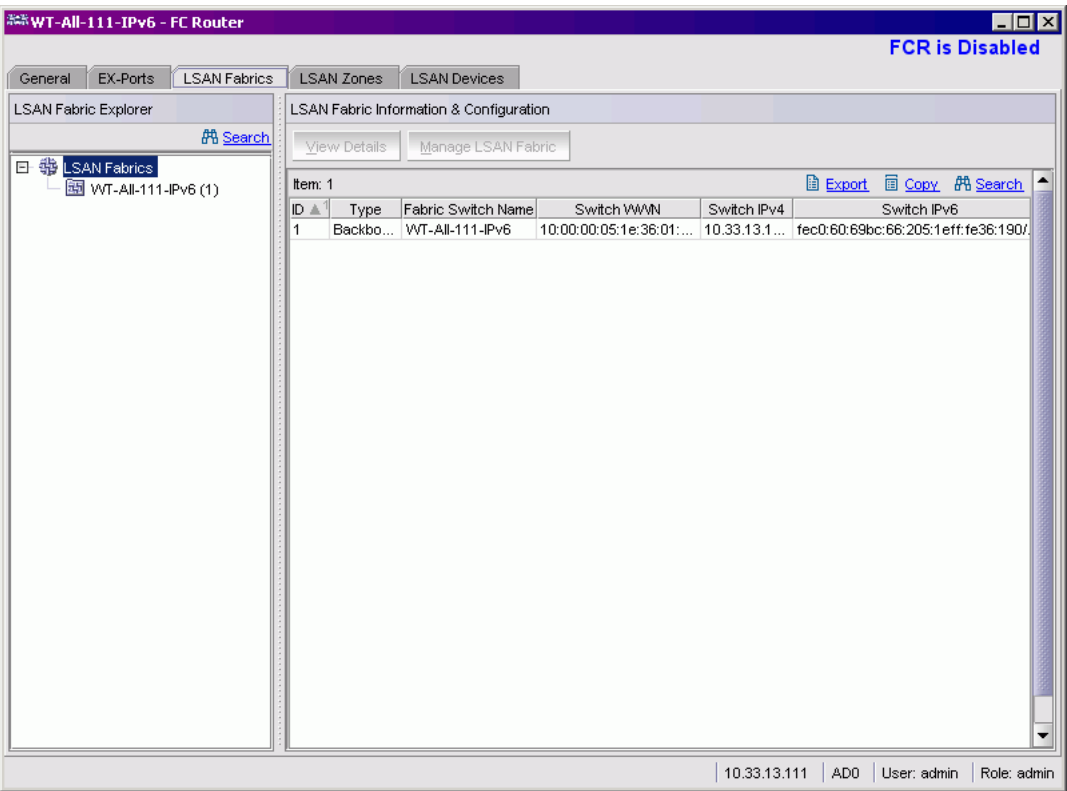


FIGURE 60 FC Routing module with LSAN Fabrics tab selected

Viewing and configuring EX_Ports

The **EX_Ports** tab (see [Figure 61](#) on page 141) displays all of the EX_Ports on the switch, including configuration and status information. The ports are sorted by slot number, and then by row number within each slot. IP addresses information is displayed in both IPv4 and IPv6 format.

NOTE

If FC Routing is disabled, then you have to disable all of the EX_Ports and you cannot enable them until FC Routing is enabled.

For more detailed information about a specific port, click a port name in the table and then click View Details in the task bar. You can also click the port name in the tree on the left side of the window.

From the **EX_Ports** tab, you can perform the following port management tasks by selecting a port in the table and then clicking a task in the task bar:

- [“To configure an EX_Port”](#) on page 141
- [“To edit the configuration of an EX_Port”](#) on page 142
- Rename an EX_Port.
- Swap the Port Index of an EX_Port (described in [“Swapping port index”](#) on page 75).

- Enable or disable an EX_Port.
- Persistently enable or disable an EX_Port.

ATTENTION

During EX_Port configuration, the port is automatically disabled, and then reenabled when the changes are applied. Be sure that you do not physically connect a port to a remote fabric before configuring it as an EX_Port; otherwise, the two fabrics merge and you lose the benefit of Fibre Channel routing.

You can enable or disable multiple ports at one time. Use Shift-click and Ctrl-click to select multiple ports in the table, and then click one of the enable or disable tasks in the task bar.

You can select multiple ports in the table, but you can select only one port at a time in the tree.

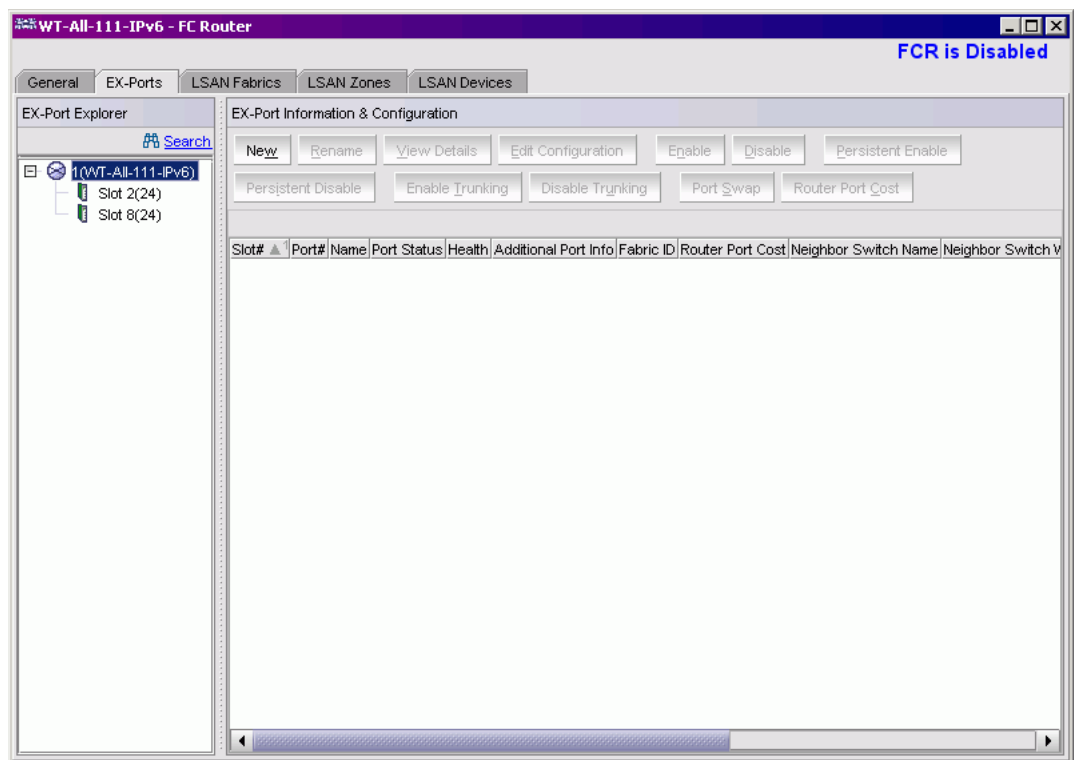


FIGURE 61 FC Routing module with EX_Ports tab selected

To configure an EX_Port

1. Launch the FC Routing module (click the **FCR** button).
2. Click the **EX_Ports** tab.
3. Click **New** in the task bar to configure one or more EX_Ports.

This launches the port configuration wizard, which guides you through the port configuration process.

4. Follow the instructions in the wizard to configure the EX_Port.

You will need to specify the Fabric ID and, if configuring an FC port, the speed and long distance mode. You can choose any unique fabric ID as long as it is consistent for all EX_Ports that connect to the same edge fabric.

To edit the configuration of an EX_Port

1. Launch the FC Routing module.
2. Click the **EX_Ports** tab.
3. Select a port to configure, by clicking in the row.
4. Click **Edit Configuration** in the task bar.

This launches the port configuration wizard, which guides you through the port configuration process.

The current configuration values are displayed in the wizard steps.

If you choose to configure a disabled port, the wizard provides the **Enable Port after configuration** check box. If you select this check box, the disabled port is automatically enabled after configuration. If you leave this box cleared, the port remains in the same state after configuration.

Viewing and configuring FCR router port cost

In FCR, EX_Ports can be assigned router port cost. The cost of the link is a positive number. The router port path or tunnel path is chosen based on the minimum cost per connection. If multiple paths exist with the same minimum cost, there will be load sharing over these paths. If multiple paths exist where one path costs lower than the others, then the lowest cost path is used.

Every link has a default cost. For an EX_Port 2Gb/sec link, the default cost is 500. For an EX_Port 1Gb/sec link, the default cost is 1000. For a VEX_Port, the default cost is 2000. If the cost is set to 0, the default cost will be used for that link.

To configure a router port cost

1. Open the Switch Administration window.
2. Click **FCR** in **Manage** section of the **Tasks** menu.
3. Click the **Ex Ports** tab.

Viewing and configuring LSAN zones

The **LSAN Zones** tab displays all the LSAN zones, in both a tabular and tree form. (If FC-FC Routing is disabled, the tables and tree nodes in this tab are empty.)

For more detailed information about a specific LSAN zone, click a zone name in the table and then click the **View Details** button in the task bar. You can also click the zone name in the tree on the left side of the window.

The LSAN matrix is mapping of LSAN Zones with the edge fabric they are going to communicate with. When an LSAN matrix is created in the backbone fabric, only the LSAN zones mapped in the edge fabrics are displayed in the LSAN Zones tab.

To share devices between any two fabrics, you must create an LSAN zone in both fabrics containing the WWNs of the devices to be shared. You create LSAN zones in the same way that you create regular zones, except for two things:

- A required name convention. The name of an LSAN zone begins with “LSAN_”. The LSAN name is case insensitive; for example, *lsan_* is equivalent to *LSAN_*, *Lsan_* and so on.
- Members must be identified by their port WWN, because PIDs are not necessarily unique across fabrics.

To enable device sharing across multiple fabrics, you must create LSAN zones on the edge fabrics (and optionally on the backbone fabric, as well), using normal zoning operations to create zones with names that begin with the special prefix “LSAN_”, and adding host and target WWNs from both local and remote fabrics to each local zone as desired. Zones on the backbone and on multiple edge fabrics that share a common set of devices will be recognized as constituting a single multi-fabric LSAN zone, and the devices that they have in common will be able to communicate with each other across fabric boundaries.

Follow the procedure described in [“Creating and populating zones”](#) on page 104 to create LSAN zones.

VIEWING LSAN DEVICES

An LSAN device can be a “physical device,” meaning that it physically exists in the fabric, or it can be a “proxy device.” A proxy device represents a real device in a remote fabric. It has a name server entry and is assigned a valid port ID. When a proxy device is created in a fabric, the real device is considered to be imported into this fabric. The presence of a proxy device is required for interfabric device communication.

The LSAN Devices tab displays information about the physical and proxy devices and displays these devices in a tree on the left side of the window. (If FC-FC Routing is disabled, the tables and tree nodes in this tab are empty.)

Click the LSAN Devices element in the tree to display a count of all the physical and proxy LSAN devices. Note that this count is for all of the LSAN fabrics.

10 Configuring the backbone fabric ID

Click the Physical Devices or Proxy Devices element in the tree to see a detailed list of the physical or proxy devices. Click the device name in the tree for more detailed information about a specific device, as shown in [Figure 62](#).

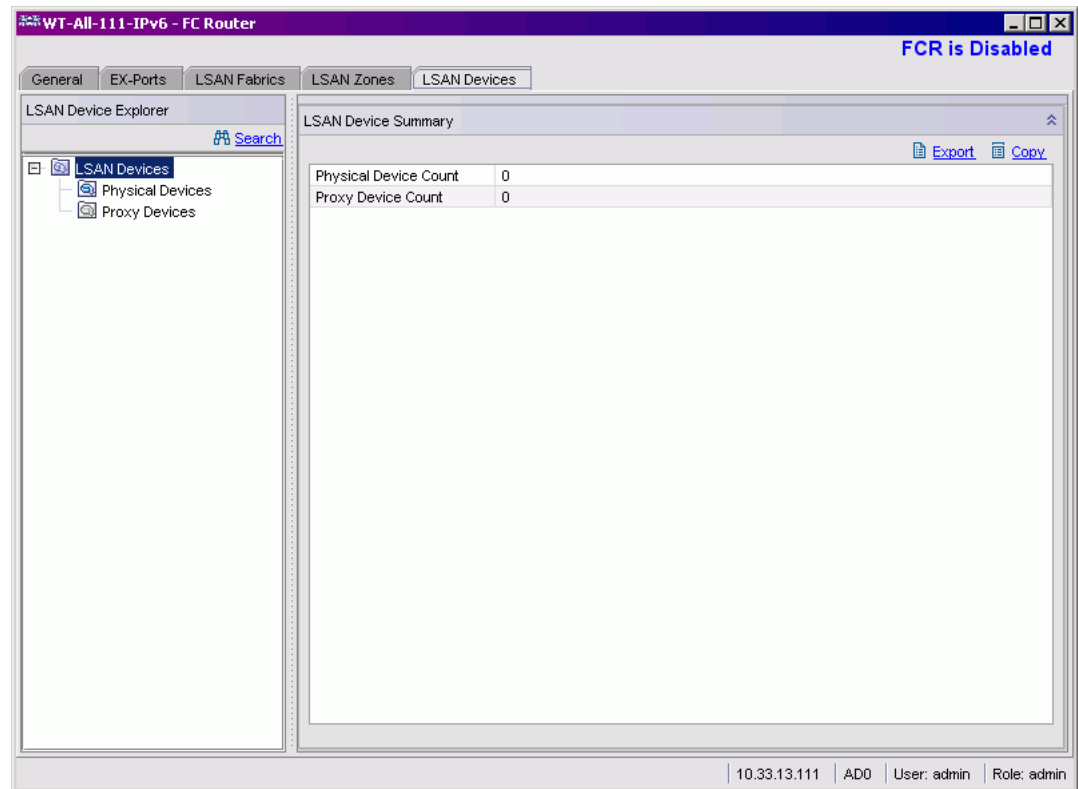


FIGURE 62 FC Routing module with LSAN Devices tab selected

Configuring the backbone fabric ID

The FC-FC Routing Service must be disabled when configuring the backbone fabric ID. Web Tools automatically disables FC-FC Routing before setting the fabric ID and then reenables it afterwards; however, you must first disable all of the EX_Ports before you invoke this operation. After the fabric ID has been changed, you can enable these ports again manually.

The fabric ID for a backbone fabric must be different than the fabric IDs of all other edge fabrics; otherwise, a fabric ID conflict error could occur.

Make sure that all switches in the backbone fabric have the same fabric ID.

To configure a backbone fabric ID

1. Open the Switch Administration window.
2. Click **FCR** in the **Manage** section of the **Tasks** menu.
3. Click the **EX-Ports** tab.
4. Disable all of the EX_Ports by selecting all of the ports in the table and then clicking **Disable**.
5. Click the **General** tab.

6. Click **Set Fabric ID** in the task bar.

The Configure Backbone Fabric ID window appears.

7. Select a fabric ID from the drop-down menu.

The fabric ID is a number from 1 through 128. Web Tools warns you if you select a fabric ID that is already in use.

8. Click **OK**.

9. Reenable all of the EX_Ports after Web Tools automatically reenables the FC-FC Routing Service.

10 Configuring the backbone fabric ID

Working With Diagnostic Features

In this chapter

This chapter contains the following information:

- [Managing trace dumps](#) 147
- [Displaying switch information](#) 149
- [Interpreting port LEDs](#) 154

Managing trace dumps

A trace dump is a snapshot of the running behavior within the Brocade switch. The dump can be used by developers and troubleshooters at Brocade to help understand what might be contributing to a specific switch behavior when certain internal events are seen. For example, a trace dump can be created each time a certain error message is logged to the system error log. Developers can then examine what led up to the message event by studying the traces.

Tracing is always “on.” As software on the switch executes, the trace information is placed into a circular buffer in system RAM. Periodically, the trace buffer is “frozen” and saved. This saved information is a “trace dump.”

A trace dump is generated when:

- It is triggered manually (use the **traceDump** command).
- A critical-level LOG message occurs.
- A particular LOG message occurs (use the **traceTrig** command to set up the conditions for this).
- A kernel panic occurs.
- The hardware watchdog timer expires.

(For information about the **traceDump** and **traceTrig** commands, see the *Fabric OS Command Reference*.)

The trace dump is maintained on the switch until either it is uploaded to the FTP host or another trace dump is generated. If another trace dump is generated before the previous one is uploaded, the previous dump is overwritten.

When a trace dump is generated, it is automatically uploaded to an FTP host if automatic FTP uploading is enabled.

11 Managing trace dumps

Using the **Trace** tab of the Switch Administration window, you can view and configure the trace FTP host target and enable or disable automatic trace uploads.

SwitchName: sw48000_wt116 DomainID: 1 VVWN: 10:00:00:60:69:e4:24:e0 Mon Apr 09 2007 17:13:35 GMT+00:00

Routing Extended Fabric AAA Service **Trace** FICON CUP ACL Distribution IPFilter IPSec Policies
Switch Network Firmware Download License User Blade Trunking SNMP Configure

Trace FTP Host

Host IP Remote Directory
User Name Password

Trace Dump Availability

Active CP 0 Standby CP 1
Trace dump generation time: Thu Mar 15 01:51:39 2007 Trace dump is not available
Trace Auto FTP Uploaded: ☐ Trace Auto FTP Uploaded: ☐

Auto FTP Upload

☐ Enable ☒ Disable

Apply Close Refresh

[Switch Administration opened]: Mon Apr 09 2007 17:11:37 GMT+00:00

Enter Host IP Address or Server Name Mode: Advanced 10.32.151.116 AD0 User: admin Role: admin

FIGURE 63 Trace tab

HOW A TRACE DUMP IS USED

The generation of a trace dump causes a CRITICAL message to be logged to the system error log. When a trace dump is detected, issue the **supportSave** command on the affected switch. This command packages all error logs, the **supportShow** output, and trace dump, and moves these to your FTP server. You can also configure your switch to automatically copy trace dumps to your FTP server (see [“Setting up automatic trace dump transfers,”](#) next).

In addition to automatic generation of trace dumps on faults, you can also generate a trace dump manually or when certain system error messages are logged. This is normally done with assistance from Brocade customer support when diagnosing switch behavior.

For details on the commands, see the *Fabric OS Command Reference*.

SETTING UP AUTOMATIC TRACE DUMP TRANSFERS

You can set up a switch so that diagnostic information is transferred automatically to a remote server. Then, if a problem occurs you can provide your customer support representative with the most detailed information possible. To ensure the best service, you should set up for automatic transfer as part of standard switch configuration, before a problem occurs.

Setting up for automatic transfer of diagnostic files involves the following tasks:

- Specify a remote server to store the files.
- Enable the automatic transfer of trace dumps to the server. (Trace dumps overwrite each other by default; sending them to a server preserves information that would otherwise be lost.)

You should also set up a periodic checking of the remote server so that you are alerted if the server becomes unavailable and you can correct the problem. See the *Fabric OS Administrator's Guide* for additional information. The following procedures describe in detail the tasks for setting up automatic transfer.

To specify a remote server

1. Open the Switch Administration window.
2. Click the **Trace** tab.
3. Type the FTP host IP address, path of the remote directory in which to store the trace dump files, FTP user name, and FTP password in the appropriate fields.

The IP address can be IPv4 or IPv6 format, or a DNS name.

The password is optional if you log in as an anonymous user.

4. Click **Apply**.

To enable automatic transfer of trace dumps

1. Open the Switch Administration window.
2. Click the **Trace** tab.
3. Select **Enable** in the **Auto FTP Upload** section to enable automatic uploading of the trace dump to the FTP host.
4. Click **Apply**.

DISABLING AUTOMATIC TRACE UPLOADS

If automatic uploading of a trace dump is disabled, you must manually upload the trace dump or else the information is overwritten when a subsequent trace dump is generated.

To disable automatic uploading of the trace dump

1. Open the Switch Administration window.
2. Click the **Trace** tab.
3. Select **Disable** in the **Auto FTP Upload** section to disable automatic uploading of the trace dump to the FTP host.
4. Click **Apply**.

Displaying switch information

This section describes how to display information about the physical components of the switch (such as fan, temperature, and power supply) as well as how to display other detailed switch information (such as firmware and IP address).

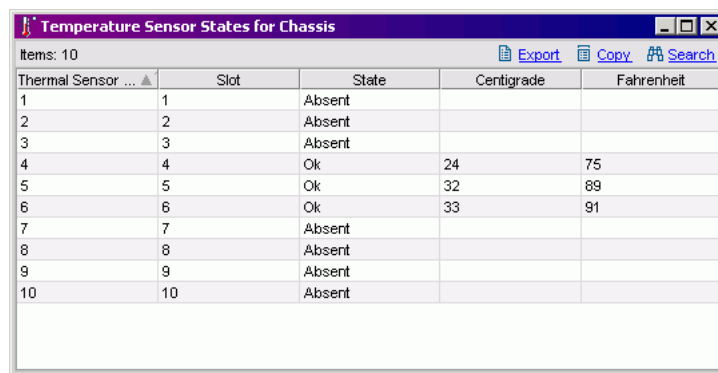
11 Displaying switch information

The Fan, Temperature, and Power Status windows have Export, Copy, and Search options at the top of the tables. These options are not available if the table does not have any content.

You must accept the Brocade Certificate at the beginning of the login to Web Tools to enable the functionality of Export and Copy.

- Click **Export** to save the contents of the table to a tab-delimited file.
- Click **Copy** to copy the contents of the table in tab-delimited text format to a file.
- Click **Search** to search for a specific text string in the table.

Type the text string in the box that displays on the table, as shown in [Figure 64](#), and press **Enter**. This is an incremental search and allows 24 maximum characters including wildcards question mark (?) and asterisk (*). The first row containing the text string is highlighted. To find the next match, hit the down arrow. To find the previous match, hit the up arrow. If the text is not found in the table, the text turns red.



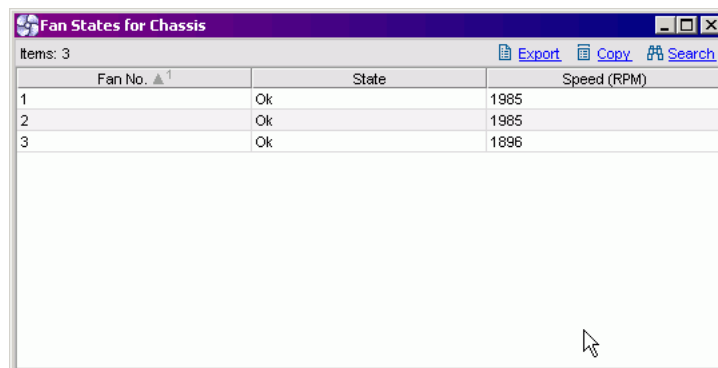
Thermal Sensor ... ▲	Slot	State	Centigrade	Fahrenheit
1	1	Absent		
2	2	Absent		
3	3	Absent		
4	4	Ok	24	75
5	5	Ok	32	89
6	6	Ok	33	91
7	7	Absent		
8	8	Absent		
9	9	Absent		
10	10	Absent		

FIGURE 64 Temperature Sensor States window

DISPLAYING DETAILED FAN HARDWARE STATUS

The icon on the **Fan** button indicates the overall status of the fans. For more information about the switch fan, refer to the appropriate hardware documentation.

You can display status information about the fans, as shown in [Figure 65](#).



Fan No. ▲	State	Speed (RPM)
1	Ok	1985
2	Ok	1985
3	Ok	1896

FIGURE 65 Fan States window

The Fan No. column indicates either the fan number or the fan FRU number, depending on the switch model. A fan FRU can contain one or more fans.

- For Brocade 24000 and 48000 directors and Brocade 4100, 4900, 5000, and 7500 switches, the Fan No. column indicates the fan FRU number.
- For Brocade 3900, the Fan No. column indicates the fan number.
- The Brocade 200E, 3250, 3850 4012, 4016, 4018, 4020, and 4024 switches do not contain fan FRUs, so for these switch models, the Fan No. column indicates the fan number.

NOTE

For these switches, if the Fan Status window has no “Fan Speed” column, *the speed is not monitored.*

To display the fan status detail

1. Select a switch from the Fabric Tree.

The selected switch appears in the Switch View. The icon on the **Fan** button indicates the overall status of the fan.

2. Click the **Fan** button.

The detailed fan status for the switch is displayed, as shown in [Figure 65](#).

DISPLAYING THE TEMPERATURE STATUS

The icon on the **Temp** button indicates the overall status of the temperature. For more information regarding switch temperature, refer to the appropriate hardware documentation.

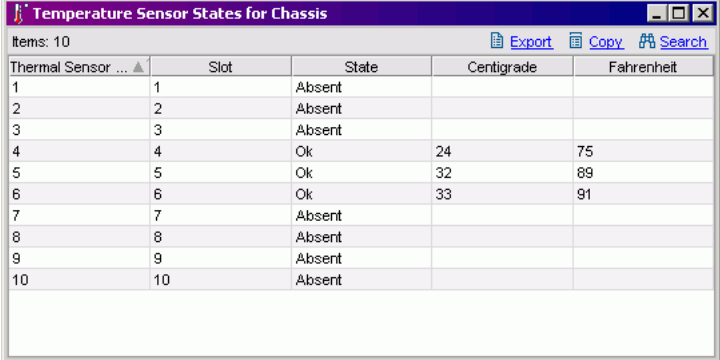
To display the temperature status detail

1. Select a switch from the Fabric Tree.

The selected switch appears in the [Switch View](#). The icon on the **Temp** button indicates the overall status of the temperature.

2. Click the **Temp** button on the Switch View.

The detailed temperature sensor states for the switch are displayed, as shown in [Figure 66](#).



Thermal Sensor ... ▲	Slot	State	Centigrade	Fahrenheit
1	1	Absent		
2	2	Absent		
3	3	Absent		
4	4	Ok	24	75
5	5	Ok	32	89
6	6	Ok	33	91
7	7	Absent		
8	8	Absent		
9	9	Absent		
10	10	Absent		

FIGURE 66 Temperature Sensor States window

DISPLAYING THE POWER SUPPLY STATUS

The icon on the **Power** button indicates the overall status of the power supply status. For more information regarding switch power modules, refer to the appropriate hardware documentation.

11 Displaying switch information

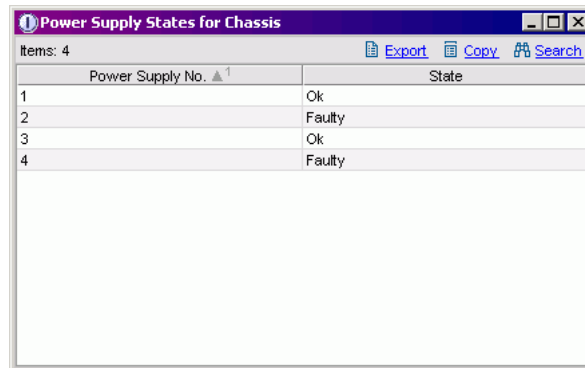
To display the power supply status detail

1. Select a switch from the [Fabric Tree](#).

The selected switch appears in the [Switch View](#). The icon on the **Power** button indicates the overall status of the power supply.

2. Click the **Power** button on the Switch View.

The detailed power supply states are displayed.



Power Supply No. ▲ ¹	State
1	Ok
2	Faulty
3	Ok
4	Faulty

FIGURE 67 Power Status window

CHECKING THE PHYSICAL HEALTH OF A SWITCH

The **Status** button displays the operational state of the switch. The icon on the button displays the real-time status of the switch.

If no data is available from a switch, the most recent background color remains displayed.

For all statuses that are based on errors per time interval, any errors cause the status to show faulty until the entire sample interval has passed.

If the switch status is marginal or critical, information on the trigger that caused that status is displayed in the Switch Information view.

Click the **Status** button to display a detailed, customizable switch status report, shown in [Figure 68](#). Note that this is a static report and not a dynamic view of the switch.

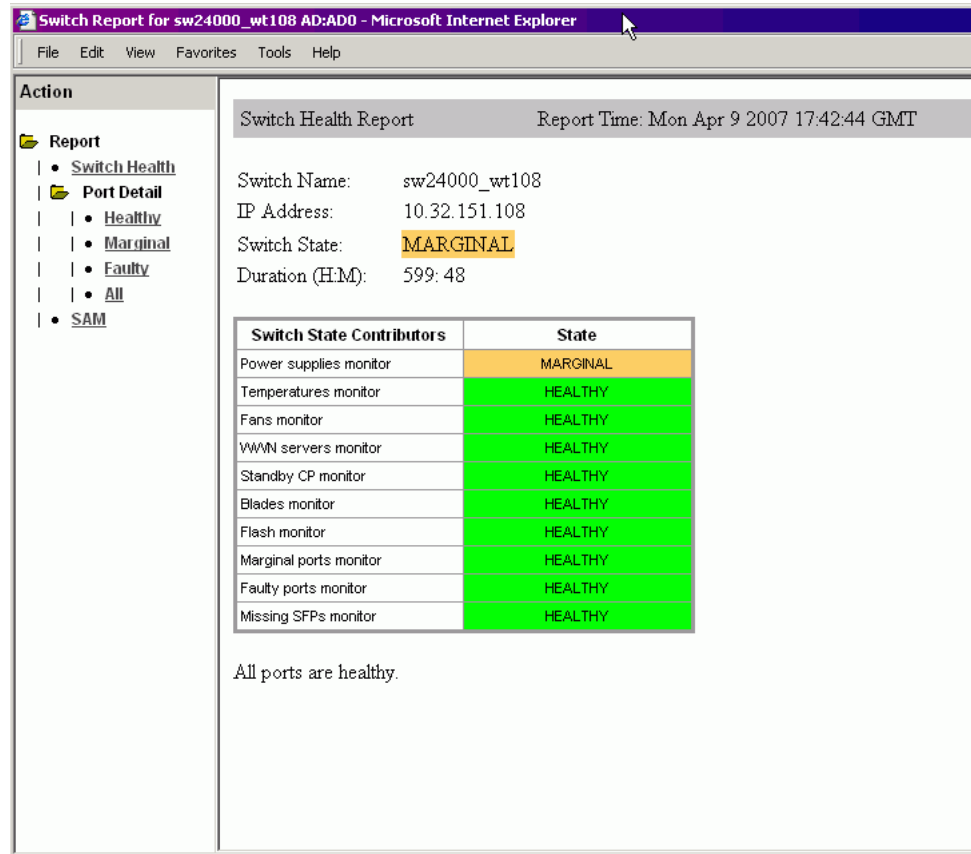


FIGURE 68 Switch Report window

To display a detailed switch status report

1. Select a switch from the [Fabric Tree](#).
The selected switch appears in the [Switch View](#). The icon on the **Status** button indicates the overall status of the switch.
2. Click the **Status** button on the Switch View.
The detailed switch health report is displayed, as shown in [Figure 68](#).
3. *Optional:* Click the underlined links in the left panel to display detailed information about ports and Switch Availability Monitoring (SAM).

NOTE

The Port Detail Report and Switch Availability Monitor (SAM) reports display the details of only those ports which are members of the current Admin Domain context and the E_Ports of the switch.

4. *Optional:* Hover the cursor over the Action bar (see [Figure 69](#)) and click an action to:
 - Refresh the information displayed in the report
 - Customize the report

11 Interpreting port LEDs

- View the data in raw XML format
- View the style sheet for the report
- View the XML schema for the report

Port #	Type	Total Up Time (Percent)	Total Down Time (Percent)	Down Occurrence (Times)	Total Offline (Percent)
048 [4/0]	U	0	0	0	100
049 [4/1]	LB	50	0	7	49
050 [4/2]	U	0	0	0	100
051 [4/3]	U	0	0	0	100
052 [4/4]	E	99	0	1	0
053 [4/5]	U	0	0	0	100
054 [4/6]	U	0	0	0	100
055 [4/7]	U	0	0	0	100
056 [4/8]	U	0	0	0	100
057 [4/9]	U	0	0	0	100
058 [4/10]	U	0	0	0	100
059 [4/11]	U	0	0	0	100
060 [4/12]	U	0	0	0	100
061 [4/13]	L	100	0	0	0
062 [4/14]	U	0	0	0	100
063 [4/15]	L	100	0	0	0

FIGURE 69 Switch Report Action menu

Interpreting port LEDs

The [Switch View](#) displays port graphics with blinking LEDs, simulating the physical appearance of the ports. One of the LEDs indicates port status; the other indicates port speed. For LED information, refer to the hardware documentation for the switch you are viewing. (The blink rate of the LEDs in the Switch View does not necessarily match the blink rate of the LEDs on the physical switch.)

NOTE

The Brocade 4900 and 7500 switches and the FR4-18i and FR4-16IP port blades do not have port speed LEDs, but only port status LEDs.

PORT ICON COLORS

The background color of the port icon indicates the port status, as follows:

- Green (healthy)
- Yellow (marginal)
- Red (critical)
- Gray (unmonitored)
- If the entire port icon is blue, the port is buffer-limited.
- If a group of port icons appears dimmed, those ports are not licensed.

LED REPRESENTATIONS

The port icons are different for different switch models. [Figure 70](#) shows E_Port port icons and associated LEDs from a Brocade 4100 switch and a Brocade 24000 director.

For the Brocade 4100, the top row of LEDs corresponds to the upper port, and the bottom row of LEDs corresponds to the lower port.

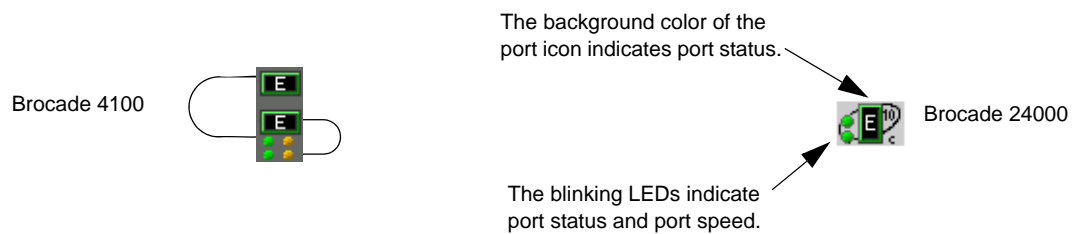
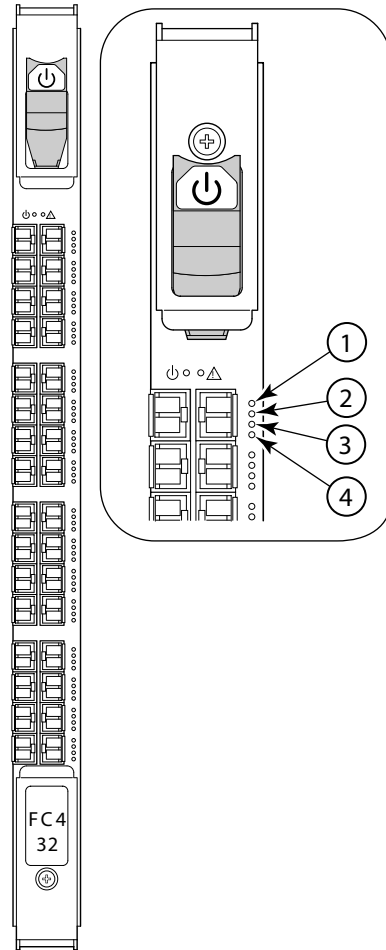


FIGURE 70 Port and LED status color-coded information in the Port icon in Switch View

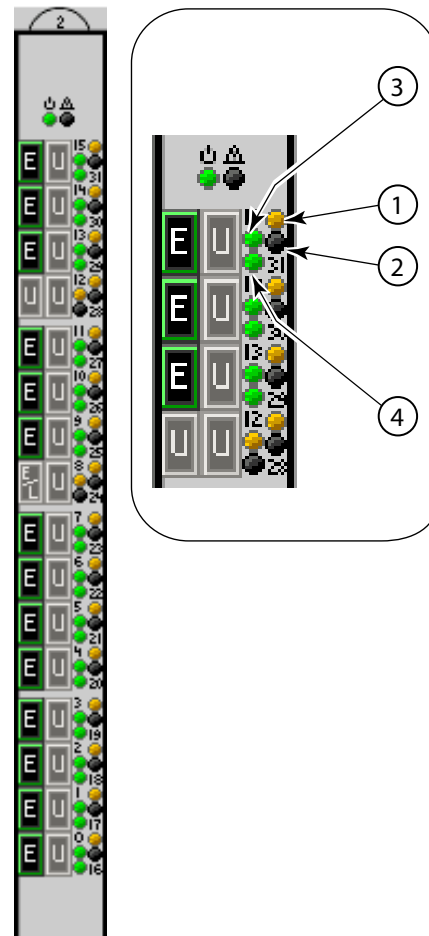
BROCADE 48000 DIRECTOR LEDS

For the Brocade 48000 director, the representation of the port LEDs on the FC4-32 port blade is not the same as the LEDs on the physical blade. [Figure 71](#) on page 156 compares the LEDs on the physical port card and the Web Tools display.

Physical Port Card



Web Tools Representation



1. Port Speed LED for the right port
2. Port Status LED for the right port
3. Port Speed LED for the left port
4. Port Status LED for the left port

FIGURE 71 Port LEDs for the FC4-32 port blade in the Brocade 48000

Administering Fabric Watch

In this chapter

This chapter contains the following sections:

- [Introduction to Fabric Watch](#) 157
- [Using Fabric Watch with Web Tools](#) 158
- [Configuring Fabric Watch thresholds](#) 159
- [Configuring alarms for FRUs](#) 162
- [Displaying Fabric Watch alarm information](#) 163
- [Configuring email notifications](#) 164

Introduction to Fabric Watch

Fabric Watch is a Brocade optionally-licensed feature that monitors the performance and status of switches. Fabric Watch can automatically alert you when problems arise, before they become costly failures.

NOTE

Fabric Watch is view-only if you do not own the switch. Owning ports on a switch is not enough to enable Fabric Watch on that switch.

To use Fabric Watch, you must have a Fabric Watch license installed on the switch.

Fabric Watch tracks a number of SAN fabric elements, events, and counters. For example, Fabric Watch monitors:

- Fabric resources, including fabric reconfigurations, zoning changes, and new logins.
- Switch environmental functions, such as temperature, power supply, and fan status, along with security violations.
- Port state transitions, errors, and traffic information for multiple port classes as well as operational values for supported models of Finisar “Smart” GBICs/SFPs.
- Performance information for AL_PA, end-to-end, and SCSI command metrics.

Fabric Watch lets you define how often to measure each switch and fabric element and allows you to specify notification thresholds. Whenever fabric elements exceed these thresholds, Fabric Watch automatically provides notification using several methods, including email messages, SNMP traps, and log entries.

For detailed information regarding Fabric Watch, see the *Fabric Watch Administrator's Guide*.

Using Fabric Watch with Web Tools

To administer Fabric Watch operations through the Web Tools Fabric Watch feature, click the **Fabric Watch** link in the **Manage** section of the **Tasks** menu.

NOTE

Unless the switch is a member of the current Admin Domain context, Fabric Watch is view-only.

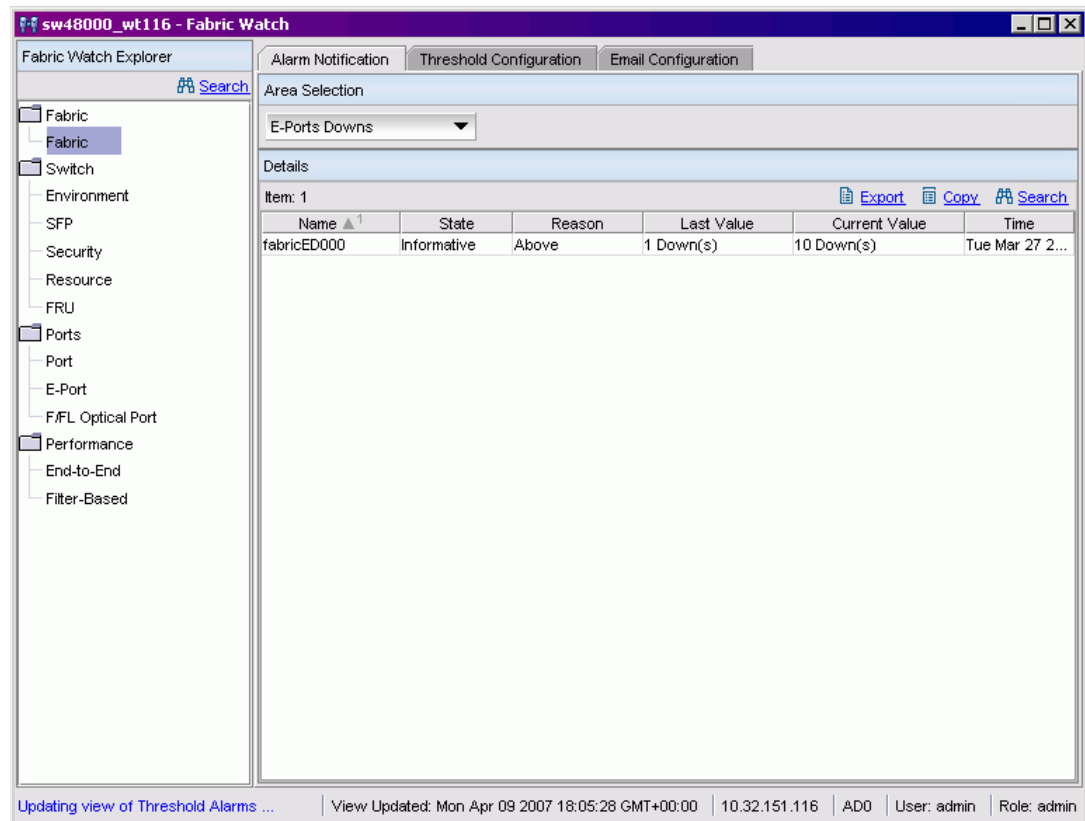


FIGURE 72 The Fabric Watch window

Fabric Watch Explorer, on the left side of the window, displays the available classes. Not all classes are available for all switches. The status bar at the bottom of the window provides you with a summary of the actions, and the date and time the module was last updated.

You should use Fabric Watch to:

- Configure custom threshold values on particular elements.
- Place limits on the acceptable values of those elements and enable the custom limits (configure threshold boundaries).
- Configure Fabric Watch to alert you to errant values.
- Configure Fabric Watch to identify unacceptable values (threshold traits).

To open Fabric Watch window

1. Select a switch from the [Fabric Tree](#) and log in if necessary.
2. Click **Fabric Watch** in the **Manage** section of the **Tasks** menu.

The Fabric Watch window opens, as shown in [Figure 72](#).

Configuring Fabric Watch thresholds

The **Threshold Configuration** tab enables you to configure event conditions. From this tab, you configure threshold traits, alarms, and email configuration.

Use the procedures in this section to configure threshold traits for all classes except for the FRU class. Use the procedure described in [“Configuring alarms for FRUs”](#) on page 162 for the FRU class.

CONFIGURING THRESHOLD TRAITS

Configure threshold traits to define a threshold for a particular class and area. You can configure the following traits for a threshold:

- Unit—The string used to define the units of measurement for the area
- Time Base—The time base (second, minute, hour, day) for the area
- Low Boundary—The low threshold for the event-setting comparisons
- High Boundary—The high threshold for the event-setting comparisons
- Buffer Size—The size of the buffer zone used in event-setting comparisons

To configure threshold traits

1. Open Fabric Watch window.
2. Click the **Threshold Configuration** tab.

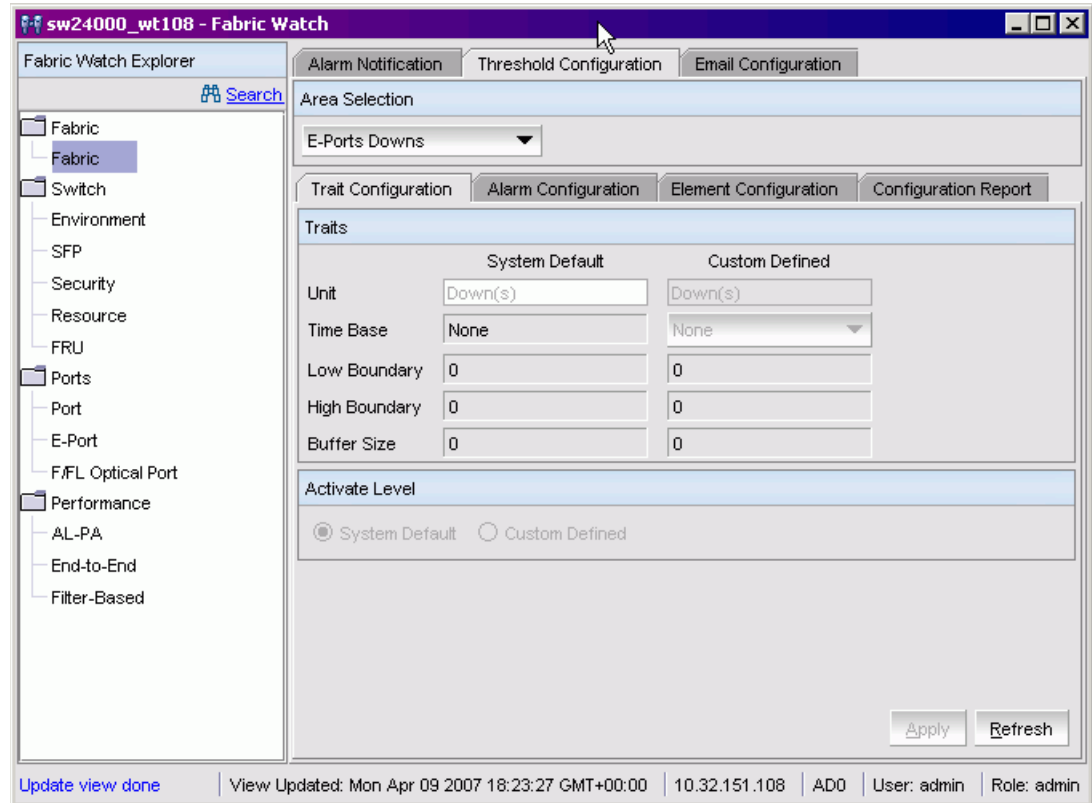


FIGURE 73 Threshold configuration in Fabric Watch

3. Click the **Trait Configuration** subtab.
4. In Fabric Watch Explorer, click a class.
5. Under Area Selection, choose an area from drop-down list.
This sets the units in the Units field.
The module displays two columns of trait information, labeled **System Default** and **Custom Defined**. You cannot modify the information in the **System Default** column.
6. In the Activate Level area:
 - Click the **System Default** radio button to use the system default settings and proceed to [step 11](#).
or
 - Click the **Custom Defined** radio button to specify new settings and proceed to the next step.
7. If necessary, select a time to record the event in the Time Base field.
8. Type the lowest boundary of the normal zone in the Low Boundary field.
9. Type the highest boundary of the normal zone in the High Boundary field.

10. Type the size of the buffer zone in the Buffer Size field.
11. Click **Apply**.

CONFIGURING THRESHOLD ALARMS

After you update the threshold information, use the **Alarm Configuration** subtab to customize the notification settings for each event setting.

To configure threshold alarms

1. Open the Fabric Watch window.
2. Click the **Threshold Configuration** tab.
3. Click the **Alarm Configuration** subtab.
4. In Fabric Watch Explorer, click a class.
5. Under Area Selection, choose an area from drop-down list.

The module displays two tables of alarm configuration information, labeled **System Default** and **Custom Defined**. You cannot modify the information in the **System Default** table.
6. In the Activate Level area:
 - Click the **System Default** radio button to use the system default settings and proceed to [step 11](#).
 - or
 - Click the **Custom Defined** radio button to specify new settings and proceed to the next step.
7. Select the check box for the type of notification method you want to use for each event type (Changed, Below, Above, Inbetween). The available alarm actions are ERROR_LOG, SNMP_TRAP, RAPI_TRAP, and EMAIL_ALERT.
8. Click **Apply**.

ENABLING OR DISABLING THRESHOLD ALARMS FOR INDIVIDUAL ELEMENTS

Use the **Element Configuration** subtab to configure element-specific alarm settings.

To enable or disable threshold alarms for an element

1. Open the Fabric Watch window.
2. In Fabric Watch Explorer, select a class.

You can set alarms for information on a switch only if that information is monitored by Fabric Watch for that switch; not all alarm options are available for all switches. For more information, see the *Fabric Watch Administrator's Guide*.
3. Click the **Threshold Configuration** tab.
4. Under Area Selection, choose the area with the alarms that you want to enable or disable.
5. Click the **Element Configuration** subtab.
6. Click an element from the Element Selection menu.
7. In the Status area:

- To disable threshold alarms, click **Disabled** and click **Apply**. The threshold alarms are disabled and you do not need to continue with this procedure.
 - To enable threshold alarms, click **Enabled** and continue with the next step.
8. Select a behavior type for the threshold alarms:
 - Click **Triggered** to receive threshold alarms only when they are triggered by events that you have defined.
 - Click **Continuous** to receive threshold alarms at a continuous interval. Select a time interval in which to receive the threshold alarms from the Time Interval menu.
 9. Click **Apply**.
 10. *Optional:* Apply the selections on this panel to multiple elements simultaneously.
 - a. Click **Apply More**.

The Multiple Selection dialog box displays.
 - b. Click the boxes next to the indices of all applicable elements.
 - c. Click **OK**.

Configuring alarms for FRUs

Configuration for the FRU class is different than configuration for the other classes. Because FRUs are not monitored through a threshold-based system, they have a simpler interface for configuration. For FRUs, you configure the *states for which an event occurs*, as described in the following procedure.

To configure alarms for FRUs

1. Open the Fabric Watch window.
2. Click the **Threshold Configuration** tab.
3. In Fabric Watch Explorer, click a FRU class.
4. Under Area Selection, choose a FRU type from the drop-down list.
5. Click the alarm states for which you want an event to register. Whenever a FRU of the selected type is detected to be in one of the selected states, an event will occur.
6. Click the methods by which you want to be notified about the FRU alarms. For FRUs, the only options are error log and email alert.
7. Click **Apply** to apply the changes to the switch.

A confirmation dialog box displays, asking if you want to apply the changes to the switch.
8. Click **OK** in the confirmation dialog box to save the changes to the switch.

Displaying Fabric Watch alarm information

From Fabric Watch, you can view two types of reports:

- Alarm notifications—Displays the alarms that have occurred for a selected class/area
- Alarm configuration—Displays threshold and alarm configurations for a selected class/area

DISPLAYING AN ALARM CONFIGURATION REPORT

Use the **Threshold Configuration** tab, **Configuration Report** subtab to display a report of the configuration for a selected class/area with the following information:

- Threshold settings (labeled **Threshold Configuration**)
- Notification settings (labeled **Action Configuration**)
- Element settings (not labeled)

You can scroll through this information but cannot make changes.

To view an alarm configuration report

1. Open the Fabric Watch window.
2. Click the **Threshold Configuration** tab.
3. Click a previously configured element from Fabric Watch Explorer (see [“Enabling or disabling threshold alarms for individual elements”](#) on page 161).
4. Under Area Selection, click the alarm area report to be viewed.
5. Click the **Configuration Report** subtab.

This tab displays a report of the configuration for the selected area.

DISPLAYING ALARMS

Using the **Alarm Notification** tab, you can view a list of all alarms that have occurred for a selected class/area (see [Figure 72](#) on page 158). [Table 9](#) describes the columns in this report. You can click the header of each column to change the way the information is sorted in your view. You can also right-click the column header and choose sort options from a menu.

NOTE

Note that for the FRU class, only the Name, State, and Time columns are displayed. In addition, if the FRU area is Fan, the Name column refers to either a fan or a fan FRU, depending on the switch model. See [“Displaying detailed fan hardware status”](#) on page 150 for more information.)

TABLE 9 Alarm notification table fields

Field	Description
Name	The string assigned to the element that had an event
State	The current state of the element
Reason	The event type that was triggered
Last Value	The data value of the element when the event was triggered
Current Value	The current data value of the element
Time	Time when the event occurred

To view alarms

1. Open the Fabric Watch window.
2. In Fabric Watch Explorer, select the class that you want to check for alarms.
3. Click the **Alarm Notification** tab.
4. In Area Selection, select the area that you want to check for alarms from the drop-down list.
All alarms for that area display.

For troubleshooting responses to alarms, see the *Fabric Watch Administrator's Guide*.

Configuring email notifications

You can be notified of an alarm condition through an email alert. If you have configured alarms to send an email notification, you must also configure the email server and the email recipient, as described in the following sections.

CONFIGURING THE EMAIL SERVER ON A SWITCH

You must set up the email notification recipient's DNS server and domain name on each switch for which email notification is enabled.

When you set up the email notification local network's DNS server and domain name for the Brocade 24000 and 48000 directors, it is on a logical-switch basis. This means that for each logical switch, you must set up the email notification recipient's DNS server and domain name individually.

To configure the email server

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **Switch** tab.
3. In the DNS Configuration area, in the DNS Server 1 field, type the primary domain Name Server IP address.

You can enter the IP address in IPv4 or IPv6 format.

4. In the DNS Server 2 field, type the secondary domain server IP address.

You can enter the IP address in IPv4 or IPv6 format.

5. In the Domain Name field, type the domain name (between 4 and 32 characters).
6. Click **Apply**.

CONFIGURING THE EMAIL ALERT RECIPIENT

You can set a different email alert configuration for each class. For example, you can set one email notification for SFPs and another for E_Ports. Before configuring email alert recipients, you must set up the email notification recipient's DNS server and domain name.

To configure the email alert alarm

1. Open the Fabric Watch window.
2. Click the **Email Configuration** tab.
3. Click the **Enable** or **Disable** radio button to enable or disable the email alert status.

When you disable email alerts, Fabric Watch does not send email notification even if the email notification method is assigned to monitored areas.

4. Type the email address of the recipient in the Recipient Email Address text box. Messages are sent to this address when email notification is enabled.

NOTE

Email addresses must not exceed 128 characters.

5. Click **Apply**.
6. *Optional:* Click **Send Test Email** to receive a test email so you can verify the email notification is working correctly. You can send a test email only after you have applied your settings.

The screenshot displays the 'Fabric Watch Explorer' window. On the left, a tree view shows the hierarchy: Fabric (selected), Switch, Environment, SFP, Security, Resource, Ports, Port, E-Port, F/FL Optical Port, Performance, End-to-End, and Filter-Based. The main area is titled 'Fabric Watch Explorer' and contains three tabs: 'Alarm Notification', 'Threshold Configuration', and 'Email Configuration'. The 'Email Configuration' tab is selected, showing the 'Email Alert Status' section with 'Enabled' selected and 'Disabled' unselected. Below this is the 'Email Information' section with a 'Recipient Email Address' text box containing 'NONE'. The 'Test Email Alert' section contains a text box with instructions and a 'Send Test Email' button. At the bottom right are 'Apply' and 'Refresh' buttons. The status bar at the bottom shows 'Update v...', 'View Updated: Tue Feb 13 2007 12:53:24 GMT+00:00', 'Host: 192.168.163.238', 'AD: AD0', 'User: admin', and 'Role: admin'.

FIGURE 74 Fabric Watch Email Configuration tab

12 Configuring email notifications

Administering Extended Fabrics

In this chapter

This chapter contains the following information:

- [“About extended link buffer allocation,”](#) next
- [“Configuring a port for long distance”](#) on page 169

About extended link buffer allocation

As the distance between switches and the link speed increases, additional buffer-to-buffer credits are required to maintain maximum performance. The number of credits reserved for a port depends on the switch model and on the extended ISL mode for which it is configured.

NOTE

Because buffer credits are a switch resource, you must own the switch in order to modify Extended Fabric settings on a port.

The **Extended Fabric** tab of the Switch Administration window displays information about the port speed, long-distance setting, and buffer credits, as shown in [Figure 75](#) on page 168. Use this tab to configure the long-distance setting of a port. For detailed information on managing extended fabrics, see the *Fabric OS Administrator's Guide*.

NOTE

You do not need to use the Extended Fabrics feature unless the link is used over long distances.

The Extended Fabric tab displays the following information:

- Port Number
- Buffer Limited—Indicates whether the port is buffer limited. A buffer-limited port can come online with fewer buffer credits allocated than its configuration specifies, allowing it to operate at a reduced bandwidth instead of being disabled for lack of buffers.

Buffer-limited operation is supported for the LO and LD extended ISL modes only and is persistent across reboots, switch disabling and enabling, and port disabling and enabling.
- Port Speed—The port speed is displayed as follows:
 - 1G—1 Gbit/sec
 - 2G—2 Gbit/sec
 - 4G—4 Gbit/sec
 - N1—Negotiated 1 Gbit/sec
 - N2—Negotiated 2 Gbit/sec
 - N4—Negotiated 4 Gbit/sec

13 About extended link buffer allocation

- Auto-Negotiation
- Buffer Needed/Allocated—The number of buffers needed and the number of buffers that are actually allocated.
- Actual Distance (km)—The actual distance for the link in kilometers.
- Desired Distance (km)—Required for a port configured in LD or LS mode (see [Table 10](#) on page 169), the desired distance, in kilometers, for the link.

For an LD-mode link, the desired distance is used as the upper limit of the link distance to calculate buffer availability for other ports in the same port group. If the measured distance is more than the desired distance, the desired distance is used to allocate the buffers. In this case, the port operates in degraded mode instead being disabled due to insufficient buffers.

For an LS-mode link, the actual distance is not measured; instead the desired distance is used to calculate the buffers required for the port.

- Long Distance—[Table 10](#) describes the long-distance settings and identifies which settings require a Brocade Extended Fabrics license.

WT_111_Saturn - Switch Administration

SwitchName: WT_111_Saturn DomainID: 111 VVNN: 10:00:00:05:1e:36:01:90 Thu May 24 2007 15:36:43 GMT+00:00

Routing Extended Fabric AAA Service Trace FICON CUP ACL Distribution IPFilter IPsec Policies Switch Network Firmware Download License User Blade Trunking SNMP Configure

Extended Fabric Administration

Items: 8

Port Number ▲1	Buffer Limited	Port Speed	Buffer Needed/Allocat...	Link Distance(km)	Desired Distance(km)	Long Distance
0	No	N4	0/0	-	N/A	L0: Normal ▼
1	No	N4	0/0	-	N/A	L0: Normal ▼
2	No	N4	0/0	-	N/A	L0: Normal ▼
3	No	N4	0/0	-	N/A	L0: Normal ▼
4	No	N4	0/0	-	N/A	L0: Normal ▼
5	No	N4	0/0	-	N/A	L0: Normal ▼
6	No	N4	0/0	-	N/A	L0: Normal ▼
7	No	N4	0/0	-	N/A	L0: Normal ▼

Slot_1 Slot_2 Slot_3 Slot_4 Slot_7 Slot_8 Slot_9 Slot_10

Apply Close Refresh

FIGURE 75 Extended Fabric tab

NOTE

In an AD that does not own the switch, only directly owned ports and E-Ports are shown. E-Ports that are not directly owned are not controllable. Long Distance configuration functionality will be available for controllable ports only, and non-owned E-Ports are viewable only.

TABLE 10 Long-distance settings and license requirements

Value	Description	Extended Fabrics License Required?
LO	No long-distance setting is enabled. The maximum supported link distance is 10 km, 5 km, or 2.5 km for ports at speeds of 1 Gbit/sec, 2 Gbit/sec, and 4 Gbit/sec, respectively.	No
LE	Extended normal setting is enabled, 10 km (6 miles) or less.	No
LD	Dynamic setting is enabled. Buffer credits for the given E_Port are dynamically configured based on the actual link distance, as long as this is less than the desired distance. If the actual link distance exceeds the desired distance, the desired distance is used to allocate the buffers. The LD-level link can operate at distances up to 500 km at 1 Gbit/sec, 250 km at 2 Gbit/sec, or 125 km at 4 Gbit/sec, depending on the switch platform and the availability of frame buffers within the port group.	Yes
LS	Static setting is enabled. Buffer credits for the given E_Port are statically configured based on the desired link distance. The LS-level link can operate at distances up to 500 km at 1 Gbit/sec, 250 km at 2 Gbit/sec, or 125 km at 4 Gbit/sec, depending on the switch platform and the availability of frame buffers within the port group.	Yes

Configuring a port for long distance

When you configure a long-distance ISL, ensure that the ports on both sides of the ISL have the same configuration, to avoid fabric segmentation.

To configure a port for long-distance connection

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **Extended Fabric** tab.
3. This step is switch-specific:

For Brocade 24000 and 48000 directors, click the slot subtab that corresponds to the correct slot for the logical switch.

For Brocade 200E, 3250, 3850, 3900, 4012, 4016, 4018, 4020, 4024, 4100, 4900, 5000, and 7500 switches, proceed directly to the next step.
4. Select a distance that corresponds to the port from the **Long Distance** drop-down menu.

Depending on the distance selected, this might require an optional license. For information about the various distances, see [Table 10](#).

If you select a long-distance setting of LD or LS, you must also type a value in the **Desired Distance** column for that port number:

13 Configuring a port for long distance

- a. Double-click the **Desired Distance** field for the port, as shown in [Figure 75](#).
- b. Type a number in the field to indicate the distance in kilometers. The allowed values depend on the port capability:
 - If the port capability is 4 GB, type a number between 10 and 125, inclusive.
 - If the port capability is 2 GB, type a number between 10 and 250, inclusive.
 - If the port capability is 1 GB, type a number between 10 and 500, inclusive.

This value is the upper limit for calculating buffer availability for other ports in the same port group. If the actual distance is more than the desired distance, the port operates in buffer-limited mode.

- c. Press **Enter** or click another port entry for the value to be accepted.
5. Click **Apply**.

Administering the iSCSI Target Gateway

This chapter describes how to use the iSCSI Target Gateway. The gateway is an intermediate device in the network, allowing iSCSI initiators in an IP SAN to access and utilize storage in a Fibre Channel SAN.

In this chapter

- [Supported platforms for iSCSI 171](#)
- [About the iSCSI service 171](#)
- [Setting up iSCSI Target Gateway Services 174](#)

Supported platforms for iSCSI

The iSCSI target gateway service is supported only on the Brocade 48000 director with CP blades running Fabric OS 5.2.0 and configured with an FC4-16IP blade (see the *Fabric OS Administrator's Guide* for more information).

About the iSCSI service

The Web Tools iSCSI Target Gateway Admin module conducts all management tasks related to the iSCSI target gateway service. Although iSCSI service is fabric wide, you can manage the iSCSI target gateway service through any iSCSI-capable switch in a fabric. Any applied iSCSI target gateway change is propagated and enforced to the whole fabric. Web Tools, as an element management tool, allows you to manage iSCSI target gateway service through one switch.

Through the iSCSI Target Gateway Admin module, you are able to conduct iSCSI target gateway-related management tasks, such as creating and managing iSCSI virtual targets, managing iSCSI sessions and iSCSI authentications, and editing discovery domains sets that enforce iSCSI device access control. The iSCSI port configuration is available to both the iSCSI Target Gateway Admin module and the port management module.

Web Tools, as a GUI-based SAN element management tool, can recognize and manage the FC4-16IP port blade in the Brocade 48000 director chassis and all Fibre Channel ports and GbE ports on the blade.

When a GbE port is configured to support iSCSI, it can transport SCSI traffic over an IP network. Each GbE port has a unique IP address called an “iSCSI target portal” and each port supports 64 iSCSI sessions. The TCP/IP stack at the port provides support for multiple TCP connections over a single GbE port.

In Web Tools, ports are addressed using slot number and port number notation (for example, 2,16).

- For Fibre Channel ports on the FC4-16IP blade, the range of ports will be 0 through 7.

- For GbE ports on the FC4-16IP blade, the port numbers shall range from ge0 through ge7. The FC4-16IP blade does not support FCIP functionality.

The iSCSI standard defines several naming conventions to enable location-independent device identification of storage resources. The FC4-16IP blade recognizes the IQN (iSCSI Qualified Name) formatted iSCSI initiator node name. For example, an iSCSI target name of “iSCSI tgt” will be presented as follows:

iqn.2002-12.com.brocade:ISCSItgt

Once an IQN is defined, you can then map LUN devices to the IQN name.

COMMON FUNCTIONS IN THE ISCSI TARGET GATEWAY ADMIN MODULE

Export, **Copy**, and **Search** links are displayed at the top of each tab.

NOTE

You must accept the Brocade Certificate at the beginning of the login to Web Tools to enable the functionality of Export and Copy.

- Click **Export** to save the contents of the table to a tab-delimited file. For CHAP, the secret is still encrypted.
- Click **Copy** to copy the contents of the table in tab-delimited text format to a file.
- Click **Print** to print out the contents of a table to a local printer.
- Click **Search** to search for a specific text string in the table.

Type a text string in the box that displays on the table, as shown in [Figure 76](#), and press **Enter**. This is an incremental search and allows 24 maximum characters including the wildcard characters: question mark (?) and asterisk (*). The first row containing the text string is highlighted. To find the next match, press the down arrow. To find the previous match, press the up arrow.

If the text is not found in the table, the text appears in red.

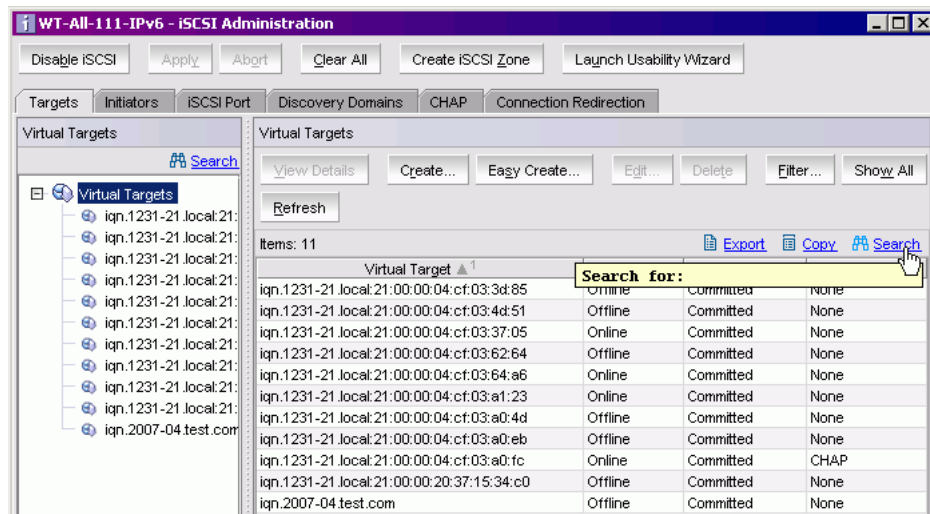


FIGURE 76 Search screen

TERMINOLOGY

iSCSI target gateway services requires you to understand some additional terminology. Following are terms that will be used in this document to explain how the iSCSI target gateway is implemented.

TABLE 11 iSCSI gateway services terminology

Term	Definition
iSCSI	Internet-SCSI. A transport carrier of the SCSI protocol over IP.
iSCSI target gateway	An intermediate device in the network that allows the iSCSI initiators in an IP SAN to access and utilize storage in a Fibre Channel SAN. the FC4-16IP embedded switch in a Brocade 48000 director functions as an iSCSI target gateway.
iSCSI port	A special GbE port used for iSCSI only. A Fibre Channel virtual initiator is created behind each iSCSI port running as a proxy Fibre Channel initiator.
iSCSI virtual target	A unique target device in the IP SAN that contains LUNs from the real Fibre Channel targets and is identified by an IQN.
iSCSI initiator	A device that begins an iSCSI transaction by issuing a command to another device (the iSCSI target), giving it a task to perform. Typically, an iSCSI host adapter is the initiator but targets can also become initiators.
iSCSI session	An iSCSI session is the basic communication “pipe” from an iSCSI initiator to an iSCSI target. A session is a group of TCP/IP connections that link an initiator with a target (loosely equivalent to a SCSI I-T nexus).
LUN mapping	Logical Unit Number mapping. The mapping of the virtual iSCSI target and the physical Fibre Channel target. One frontend LUN (VT LUN) maps to a backend LUN (Fibre Channel LUN). The frontend LUN numbers can be different from the backend LUN numbers.
Fibre Channel LUN	The LUN identifier of the Fibre Channel target.
VT LUN	Virtual target LUN. The LUN identifier of the iSCSI virtual target.
Fibre Channel virtual initiator	(FC-VI) The iSCSI port looks like an F_Port to the rest of the system. There is one Fibre Channel virtual initiator per iSCSI. The Fibre Channel proxy initiator solution is used. FC-VI registers to the Name Server with its symbolic port name (PWWN) and node name (NWWN). The FC-VI in the Name Server entry is created irrespective of the host connectivity.
discovery domain (DD)	Created between an iSCSI host and iSCSI targets using their IQN for the purpose of iSCSI device access control.
discovery domain set (DDSet)	Created using DDs. Can be configured to enable or disable the configuration for the purpose of iSCSI device access control.
CHAP authentication	Authenticates the initiators against a list of user names and passwords with CHAP (Challenge Handshake Authentication Protocol) authentication in either one-way or mutual.
IQN	An iSCSI Qualified Name that indicates an iSCSI node name in a form that is of human readable notation using the following syntax: iqn.yyyy-mm.<reverse of DNS>:<optional iSCSI unique string>
GbE port	Gigabit Ethernet port. Uses a copper CAT-5e cable for an IP connection to an RJ-45 copper connector. FC4-16IP has 8 ports of this type that support 1 Gbps speed.
PDU	Protocol Data Unit. A unit of data with a header and an optional data section.

For additional information about iSCSI target gateway, see the *Fabric OS Administrator's Guide*.

SAVING CHANGES

There are several ways to save changes on the switch and apply them to the fabric (applies to the iSCSI Target Gateway Admin module only):

- **Apply**—Click **Apply** and your changes will be transferred from the Web Tools database to the switches database and distributed throughout the fabric.
- **Abort**—Click **Abort** to cancel the changes before saving them. The configuration is restored to the last saved data point.
- **Clear All**—The **Clear All** button, located in the menu bar of the iSCSI module, has the ability to clear all parameters of the iSCSI target gateway databases, including virtual targets, iSCSI initiators, discovery domains, discovery domain sets, and all CHAP users and associated secrets. The IP interface information, however, is not deleted.

ATTENTION

The **Clear All** button deletes the information from the database. Before you use the **Clear All** function, perform a **configUpload** and save a backup of the iSCSI target gateway database.

Setting up iSCSI Target Gateway Services

The following procedure provides an overview of the basic steps for setting up iSCSI target gateway services. The iSCSI Setup wizard guides you through the steps to set up iSCSI connectivity between IP networks and your Fibre Channel SAN.

Click the Launch Usability Wizard button on the iSCSI Administration window to use the iSCSI Setup wizard to perform all setup tasks.

You can also perform these tasks from the iSCSI Administration window:

- [“Activating the iSCSI Feature”](#) on page 176
- [“Configuring the IP Interface”](#) on page 176
- [“Managing the iSCSI Virtual Targets”](#) on page 179 (to create iSCSI virtual targets from physical Fibre Channel targets)
- [“Managing Discovery Domains”](#) on page 182 (to allow all iSCSI ports to access to Fibre Channel physical targets)
- [“Managing Discovery Domains”](#) on page 182 (to manage iSCSI device access control through creating and enabling discovery domain sets)
- [“Configuring CHAP”](#) on page 185 (to define access to log in to virtual targets through the Microsoft iSCSI Initiator.)
- [“Configuring an iSCSI Fibre Channel Zone”](#) on page 187)

ATTENTION

After mapping iSCSI targets, do not move the targets out of ADO by adding them to other Admin Domains unless you first explicitly add them back to ADO.

LAUNCHING THE ISCSI TARGET GATEWAY ADMIN MODULE

When you click **iSCSI** in the **Manage** section of the **Tasks** menu, the iSCSI Administration window opens. This option is available on all Brocade 48000 switches with option 5 configured and without a FC4-16IP blade.

NOTE

Since the entire fabric is scanned when you open the iSCSI Administration window, larger fabrics may take longer to load.

The Target Group is the first pane that comes up and presents all the iSCSI virtual targets and their mapping to the Fibre Channel targets (physical and virtual) from the fabric. You can create and add LUNs to the existing iSCSI virtual targets from this group.

When you select an IQN you have the ability to edit or delete virtual targets associated with that IQN. You can view current sessions and discovery domain accessibility.

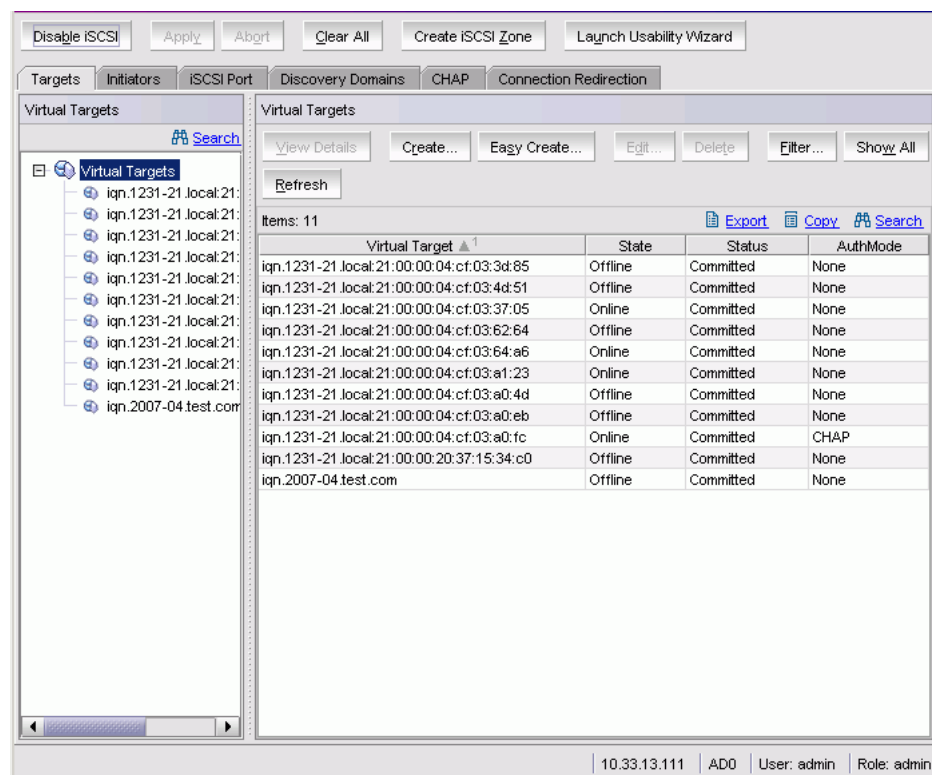


FIGURE 77 iSCSI Target Gateway Admin with the Targets tab selected

To launch iSCSI Target Gateway Admin

1. Select a switch from the [Fabric Tree](#) and log in, if necessary.

The selected switch appears in [Switch View](#).

Make sure that your Admin Domain Context is either ADO or AD255.

Generally, the default user Admin Domain is ADO. The recommended practice is to perform all iSCSI management from ADO; you can make changes from AD255 but you will not be able to make any zoning changes.

2. Click **iSCSI** in the **Manage** section of the **Tasks** menu.

iSCSI Administration window opens.

NOTE

If the iSCSI Target Gateway Services is disabled, you must click the Enable iSCSI button at the top of the window to enable the services.

To launch the iSCSI Setup wizard

1. Select a switch from the [Fabric Tree](#) and log in, if necessary.

The selected switch appears in [Switch View](#).

Make sure that your Admin Domain Context is either ADO or AD255.

Generally, the default user Admin Domain is ADO. The recommended practice is to perform all iSCSI management from ADO; you can make changes from AD255 but you will not be able to make any zoning changes.

2. Click **iSCSI** in the **Manage** section of the **Tasks** menu.

iSCSI Administration window opens.

3. Click the **Launch Usability Wizard** button.

Follow the steps in the wizard to complete all the setup tasks.

ACTIVATING THE iSCSI FEATURE

A director by default has iSCSI disabled. If a switch has iSCSI disabled or there is no iSCSI virtual target created yet, WebTools assumes that iSCSI has not been activated.

To activate the iSCSI Feature

1. Ensure that the blade is inserted in the director and powered on.
2. Open iSCSI Target Gateway Admin as described on [page 175](#).
3. Click **Enable iSCSI**.
4. Click **Apply**.

CONFIGURING THE IP INTERFACE

This step configures iSCSI ports (GbE Ports) found on the FC4-16IP. You must have at least one iSCSI port configured to log into the iSCSI target.

There are two steps in this process:

- Configure the IP interface for iSCSI port.
- Configure the IP route for the iSCSI port.

The iSCSI Port Group tab allows you to configure iSCSI ports, displays session details on a port, and shows the port statistics. It also allows you to view and configure the IP interface and routes that are located on the IP Interface tab. You can edit or delete the IP address, but you cannot add any additional IP addresses to this interface.

When you select the switch in the left pane, the right pane lists the tasks you can perform on that switch in relation to one of the GbE ports.

When you select one of the GbE ports, you can perform the same tasks listed previously: view and capture statistics related to the port, add or delete IP addresses, add or delete IP routes, view current sessions, and view the iSCSI statistics in brief.

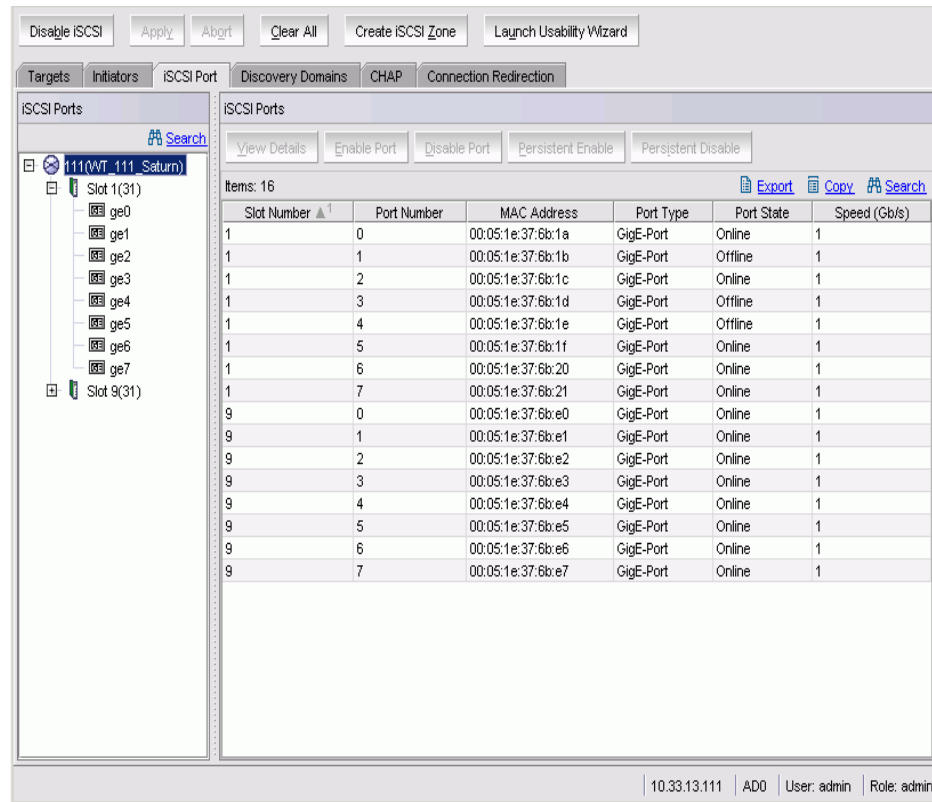


FIGURE 78 iSCSI Port tab

If an IP address or IP route is already configured on the GbE port, then it will not be editable as any edits will disrupt any iSCSI traffic.

Configuring the IP route is optional because when an IP address is set up, a route is automatically set up as well.

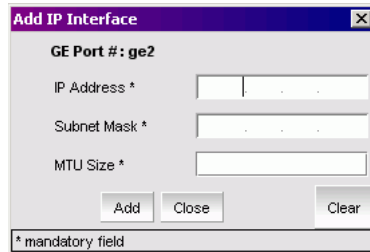
To configure the IP address

1. Open iSCSI Target Gateway Admin as described on [page 175](#).
2. Select the **iSCSI Port** tab.
3. In the left pane, select the GbE port that will be used.
4. Select the **IP Interface** subtab and click **Add**.
5. Enter the IP address and subnet mask.
6. Enter the MTU size or accept the default MTU size and click **Add**.

To edit an IP Address

1. Launch the iSCSI Target Gateway Admin module as described on [page 175](#).
2. Select the **iSCSI Port** tab.

3. From the left pane, select the GbE port that will be used.
4. Select the **IP Interface** subtab and select the item on the tab.
5. Click **Edit**.
6. Click **OK** when you receive the Warning dialog box.



The 'Add IP Interface' dialog box has a title bar with a close button. It contains a label 'GE Port #: ge2'. Below it are three input fields: 'IP Address *', 'Subnet Mask *', and 'MTU Size *'. Each field has a small icon to its right. At the bottom are three buttons: 'Add', 'Close', and 'Clear'. A legend at the bottom left indicates '* mandatory field'.

FIGURE 79 Edit IP Interface dialog box

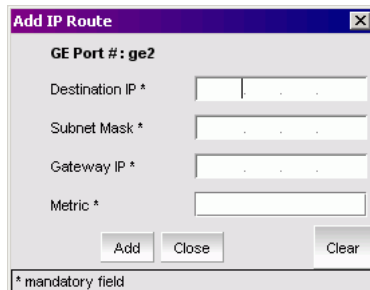
7. Enter the subnet mask.
8. Enter the MTU size or accept the default MTU size and click **OK**.

NOTE

To change the IP address, delete the current IP address and re-create it. You will not be allowed to create an additional IP address *for this interface*, as there can be only one IP address per interface.

Optional: To configure the IP route

1. Launch the iSCSI Target Gateway Admin module as described on [page 175](#).
2. Select the **iSCSI Port** tab.
3. From the left pane, select the GbE port that will be used.
4. Select the IP Routes tab.
5. Click **Add**.



The 'Add IP Route' dialog box has a title bar with a close button. It contains a label 'GE Port #: ge2'. Below it are four input fields: 'Destination IP *', 'Subnet Mask *', 'Gateway IP *', and 'Metric *'. Each field has a small icon to its right. At the bottom are three buttons: 'Add', 'Close', and 'Clear'. A legend at the bottom left indicates '* mandatory field'.

FIGURE 80 Add IP Route dialog box

6. Enter the IP address, subnet mask, and gateway IP address, and the metric.
7. Click **Add**.

To edit the IP route

1. Open iSCSI Target Gateway Admin as described on [page 175](#).
2. Select the **iSCSI Port** tab.
3. From the left pane, select the GbE port that will be used.
4. Select the **IP Routes** tab.
5. Click **Edit**.

A warning dialog box appears.

6. Click **OK**.
7. Enter a new value for the metric.
8. Click **OK**.

If you want to change a value other than the metric, you will need to delete this route and create another in its place.

MANAGING THE ISCSI VIRTUAL TARGETS

iSCSI virtual target creation is the first pane in the iSCSI Target Gateway Admin module. The iSCSI Virtual Target wizard provides two ways to create iSCSI targets: Create and Easy Create. Both procedures are simple to use, but Create allows you to double check your work several times before committing the changes.

You can edit a virtual target even when there is an active iSCSI session.

To create iSCSI virtual targets

1. Open iSCSI Target Gateway Admin as described on [page 175](#).
2. Select the **Targets** tab.
3. Click **Create**.

The VT Configuration Wizard opens.

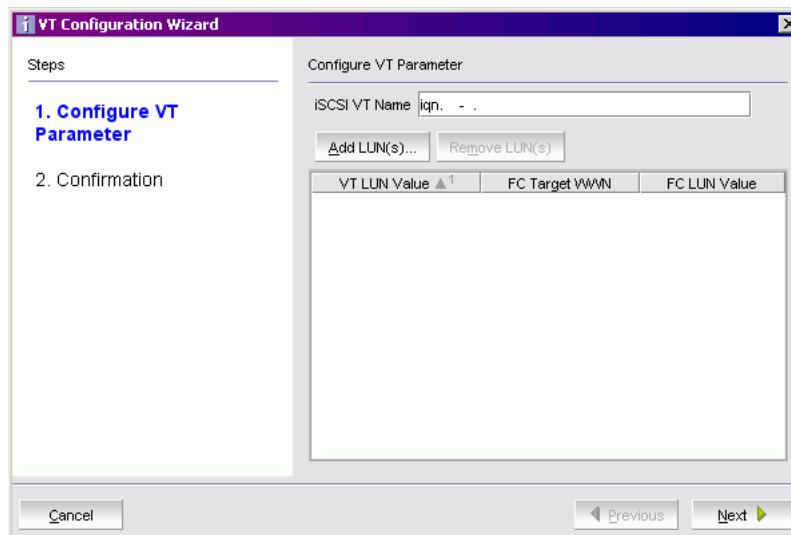


FIGURE 81 VT Configuration Wizard

4. Enter an IQN.
The text field will display the value “iqn” and you need to enter the remaining data.
5. Click **Add LUNs**.
6. On LUN Addition Dialog, select LUNs to add.
You will need to expand each unit until you get to the actual LUN.
7. Click **Add LUN(s)**.
This will add the selected LUNs to your virtual target.
8. Click **Next** and click **Finish**.

To use Easy Create

1. Open iSCSI Target Gateway Admin as described on [page 175](#).
2. Select the **Targets** tab.
3. Click **Easy Create**.

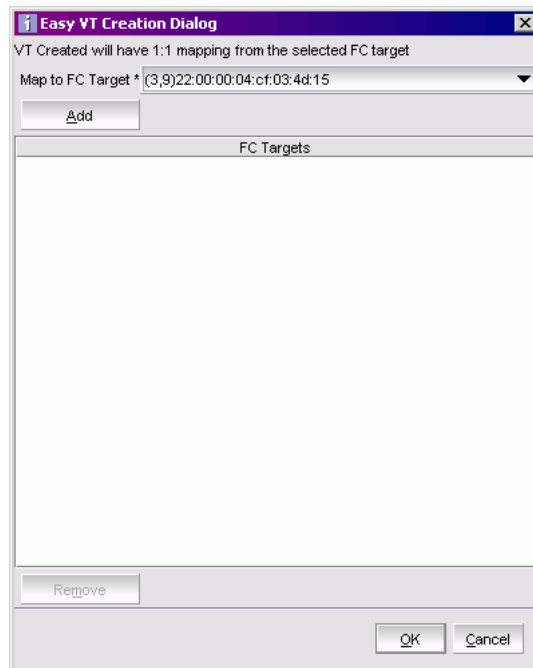


FIGURE 82 Easy VT Creation Dialog

4. Follow the instructions in the wizard to create a virtual target in iSCSI.
The wizard is self-explanatory, so the individual steps are not described in this document.

NOTE

When you click **Add** in the Easy VT Creation dialog, virtual targets are created for all the available physical targets in a 1:1 combination. If you add the virtual target using the **Add** button and click **OK**, the virtual target will be created for only the physical targets that were selected.

To edit an iSCSI Target

1. Open iSCSI Target Gateway Admin as described on [page 175](#).
2. Select the **Targets** tab.
3. Select the IQN in the left pane of where you want to edit the targets.
4. Click **Edit**.

The VT Configuration wizard opens.

5. Follow the instructions in the wizard to edit an iSCSI virtual target.

The wizard is self-explanatory, so the individual steps are not described in this document.

NOTE

The **Remove LUN(s)** button is available only for virtual targets that have not been fully initialized as a target.

To search for a specific Fibre Channel target in the Creation wizard

1. Click the **Search** link.
2. Input the <domain,port>, partial WWN, or vendor name, or a combination of these values.
3. Click **Next**.

The search result will be shown as selected nodes in the Fibre Channel target tree. No changes will be made if search criteria do not match.

VIEWING ISCSI INITIATORS

When you set up the iSCSI target gateway on a switch, all initiators may not be online yet, but the initiators will automatically be picked up and displayed in the **Initiators** tab. The table size grows automatically to show the initiators.

This view presents all iSCSI initiators (hosts) and their associated mappings. You can view iSCSI initiator sessions here.

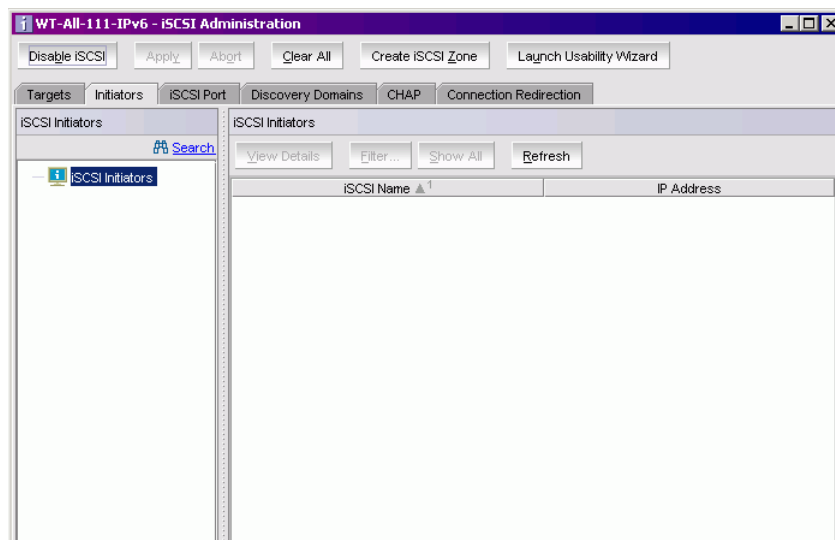


FIGURE 83 Initiator group

MANAGING DISCOVERY DOMAINS

In this step, you configure discovery domains and discovery domain sets for managing iSCSI device access control. The Discovery Domains pane displays all discovery domains and discovery domain sets and allows you to manage them.

When you select **DDInfo** in the tree in the left pane, you can create a discovery domain. If you select an object in the discovery domain set listed you can view, create, edit, delete, enable, or disable any of the discovery domain information contained in each object. If you select a discovery domain object, you can edit or delete the data contained in the object.

Discovery domains are placed in a discovery domain set.

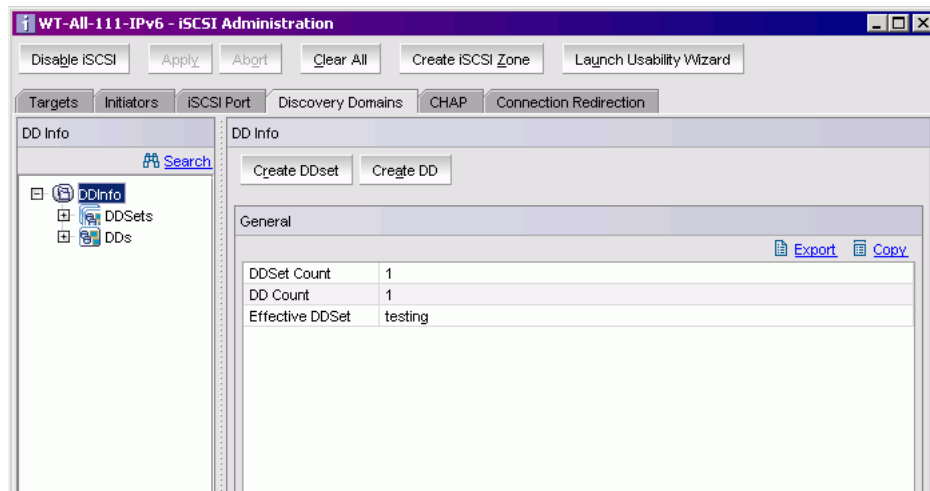


FIGURE 84 Discovery Domain group

About Discovery Domains (DD)

In the Create DD wizard you can configure the DD, add DDs to DDSets, and view the confirmation report.

NOTE

When you create new DDs, you specify a DD name, but you cannot edit or change the name when you edit the DDs.

When you launch the DD or DDSet wizard, you can add or remove virtual targets to the selected DD or DDSet. The wizard displays all available initiators and targets grouped by initiators and targets on the left side. Depending on how the wizard is launched, the right side will be blank or list current members of the DD being used:

- When the wizard is launched using **Create**, the list at the right is blank.
- When the wizard is launched using **Edit**, the list at the right displays current members of the DD being viewed.

Discovery domains can be created with virtual targets, iSCSI initiators, or both.

In the wizard:

- You can configure the DD. You specify the DD name, and then you can add or remove initiators and targets. You can also add any offline device(s) by entering the IQN name in the IQN name field and clicking **Add Offline Devices** under the list on the right. The offline device name will be added to the Selected List.
- You can also filter out initiator and targets from the tree in the Selection List by using the **Filter** button. You can enter the full or partial name of an iSCSI member in the IQN Name text box and clicking the **Filter** button. Based on the filter criteria, the tree will display only those members satisfying the filter criteria. You then add the device by selecting the device and clicking the **Add** button. In order to view the all available initiators and targets, click **Show All**.

To create a discovery domain

1. Open iSCSI Target Gateway Admin as described on [page 175](#).
2. Select the **Discovery Domains** tab.
3. Click **Create DD**.

The Create DD wizard opens.

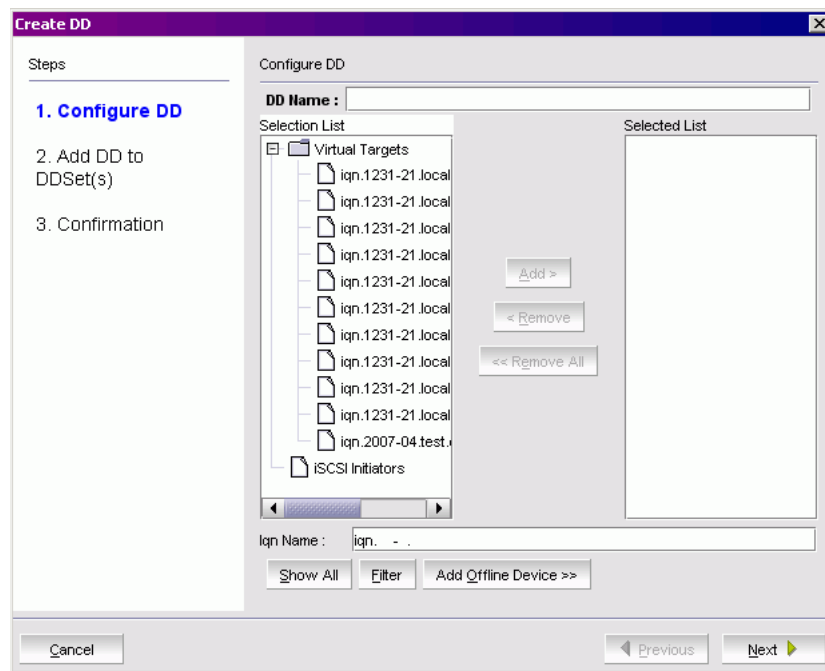


FIGURE 85 Create DD wizard

4. Follow the instructions in the wizard to create an iSCSI discovery domain.

The wizard is self-explanatory, so the individual steps are not described in this document.

To edit a discovery domain

1. Open iSCSI Target Gateway Admin as described on [page 175](#).
2. Select the **Discovery Domains** tab.
3. Select a DD in the left pane and click **Edit**.

4. Select virtual targets and use the buttons to add or remove them from the DD.
5. Click **Next**.

The opening screen with a list of virtual targets that you added to your DDs is displayed.

6. Click **Next**.

You can verify the virtual targets that you added to your DDs.

7. Click **Finish**.

You can confirm the changes that you made before committing them.

About discovery domain sets (DDSet)

The iSCSI Target Gateway Admin module provides you with the flexibility to create discovery domain sets (DDSet) that define the host target access. (This functionality is similar to Fibre Channel zoning.) Use the **Discovery Domains** tab to view and manage access from iSCSI initiators to iSCSI virtual targets.

The DD view displays all DDSets created and allows you to create, edit, enable, or disable a discovery domain set. Select a DDSet from the left pane to view the contents of the set.

Discovery domains can be created but they do not have to be associated with a DDSet. However, a DDSet cannot be created without having at least one discovery domain associated in it. Only floating discovery domains are allowed.

NOTE

You cannot rename a discovery domain or discovery domain set.

To create a discovery domain set

1. Open iSCSI Target Gateway Admin as described on [page 175](#).
2. Select the **Discovery Domains** tab
3. Click **Create DDSet**

The Create DDSet wizard opens.

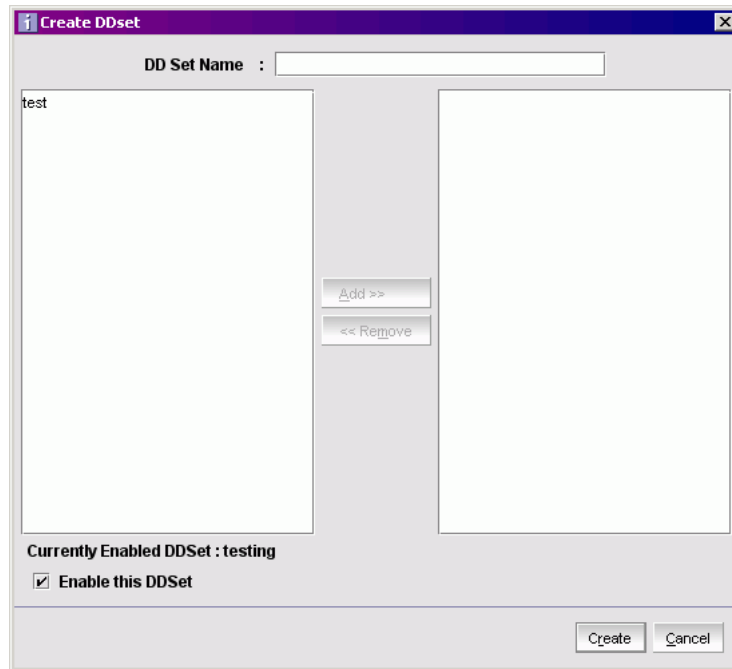


FIGURE 86 Create DDSet wizard

4. Follow the instructions in the wizard to create an iSCSI discovery domain set
The wizard is self-explanatory, so the individual steps are not described in this document.

To edit a Discovery Domain Set

1. Launch the iSCSI Target Gateway Admin module as described on [page 175](#).
2. Select the **Discovery Domains** tab.
3. Select a DDSet in the left pane and click **Edit**.
4. Select the discovery domains to add to or remove from the DDSet.
5. Click **Finish**.

You can confirm the changes that you made.

CONFIGURING CHAP

This view allows you to define access to login to that virtual target through the Microsoft iSCSI Initiator. You can create, view, and change CHAP users and their associated secrets. Once a CHAP user is created, you can modify only the CHAP secret.

The CHAP module pane lists CHAP secrets in a table with the user name and chap secret in encrypted format (*). You can add, delete, or modify CHAP entries. Each CHAP secret has:

- User name maximum length of 255 characters
- CHAP secret of maximum length of 63 characters

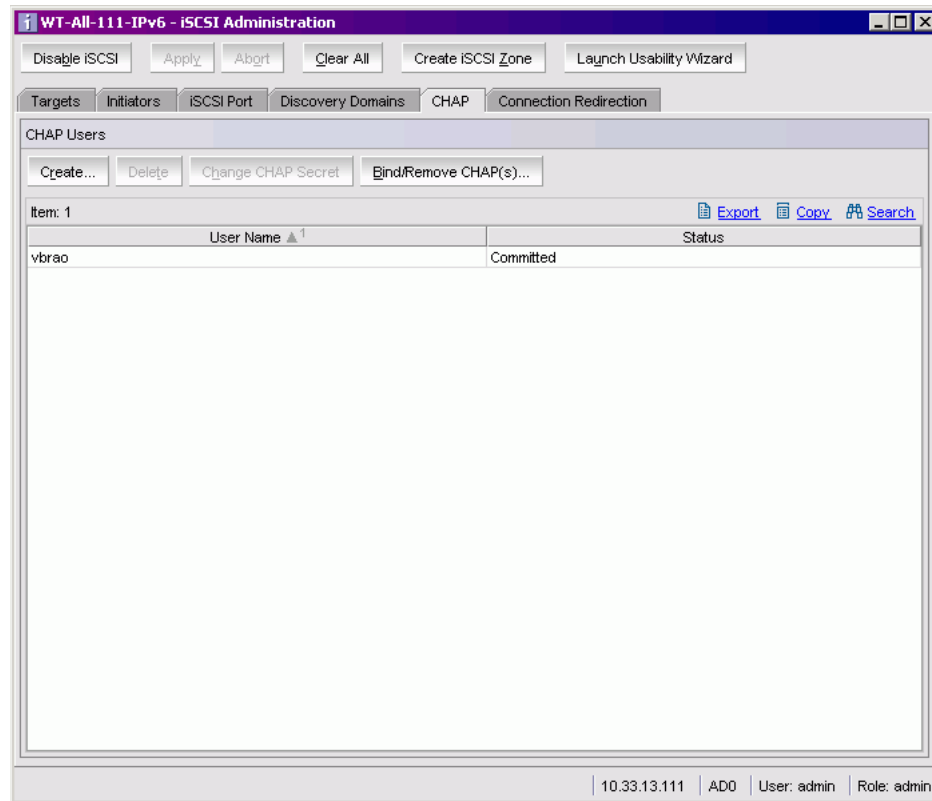


FIGURE 87 CHAP tab

To create a CHAP user

1. Launch the iSCSI Target Gateway Admin module as described on [page 175](#).
2. Select the **CHAP** tab.
3. Click **Create**.
4. Enter the CHAP user name.
Optional: To add more than one user at a time, click **Add**.
5. Enter a CHAP secret and click **Apply**.

To edit a CHAP secret

1. Launch the iSCSI Target Gateway Admin module as described on [page 175](#).
2. Select the **CHAP** tab.
3. Click **Change CHAP Secret**.
You can edit the CHAP secret but not the CHAP user name.
4. Fill in the fields in the dialog box to edit a CHAP secret.

To bind or remove CHAP users

1. Launch the iSCSI Target Gateway Admin module as described on [page 175](#).
2. Select the **CHAP** tab.
3. Click **Bind/Remove Chap(s)**.
4. Select a virtual target
5. Enter a new CHAP user, if necessary.
6. Select the CHAP users and click **Add** or **Remove** to move them into the appropriate list (unassociated or associated CHAP users).
7. Click **Apply**.

CONFIGURING AN ISCSI FIBRE CHANNEL ZONE

After you have finished setting up the iSCSI target gateway and whenever you later modify the iSCSI virtual target mappings, you must create an iSCSI Fibre Channel zone to allow the system's virtual initiators (logical FC devices that represent iSCSI initiators) to communicate in a zoned FC environment with the physical devices to which you have mapped the iSCSI virtual targets.

The procedures in this section show you how to create this zone and add it to the fabric's zone database.

- If you already have zone configurations defined in your fabric, you will also be able to add the zone that you create here to some or all of these configurations by selecting them from a list.
- If a defined configuration is currently effective in the fabric and you add your iSCSI FC zone to that configuration, the configuration is automatically re-enabled to include this zone.

NOTE

If you do not have a zoning license or no zoning implemented, you do not need to create one for iSCSI target gateway service.

The following default zoning conditions apply:

- If default zoning is set to No Access, then creating an iSCSI Fibre Channel zone is mandatory as there is no way for the devices to talk to each other without one.
- If default zoning is set to All Access and no effective zone configuration, then you can create an iSCSI Fibre Channel zone and add it to a defined configuration, but you do not need to enable the defined configuration. Since your default zoning is All Access with no effective zone configuration, all devices can already talk to each other. However, to avoid SAN congestion in the future, you should implement a zoning plan for your devices.

Use the Zone Admin module to create zoning or remove or add zone members to reflect your iSCSI devices.

For more information about configuring zones, see [“Configuring zoning”](#) on page 96.

To create an iSCSI Fibre Channel zone with no effective zone configuration

1. Open iSCSI Target Gateway Admin as described on [page 175](#).
2. Click **Create iSCSI Zone**.

The following dialog box is displayed.

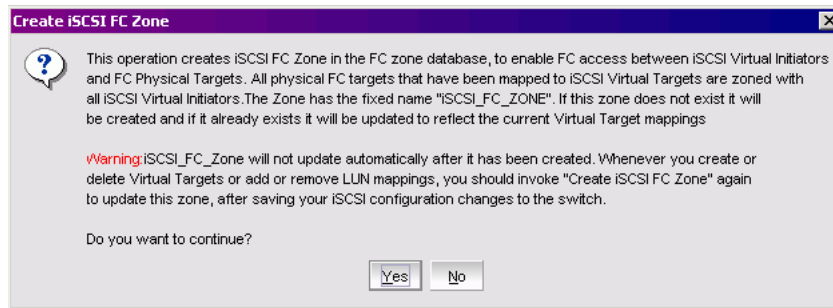


FIGURE 88 Create an iSCSI FC zone dialog box

3. Click **Yes**.

The Create iSCSI Zone wizard creates a zone called “ISCSI FC ZONE,” which will not be placed into a defined configuration or automatically enabled.

4. Add the ISCSI FC ZONE into a configuration.

See [“Creating zone configurations”](#) on page 107.

To create an iSCSI Fibre Channel zone with an effective zone configuration

1. Launch the iSCSI Target Gateway Admin module as described on [page 175](#).
2. Click **Create iSCSI Zone**.
3. Click **Yes**.
4. Select a configuration in the dialog box.
 - If you select a non-effective configuration, the iSCSI Fibre Channel zone will be added into that configuration. The configuration will not be re-enabled and will remain in the defined configuration until you enable it. You will need to add the iSCSI Fibre Channel zone to the effective configuration at a later date or iSCSI target gateway will not work.
 - If you select an effective configuration, the iSCSI Fibre Channel zone will be added into the effective configuration and then the configuration will be re-enabled. This affects the entire SAN; the zoning database needs to update itself and then replicate its changes into the fabric.

ATTENTION

Schedule your changes during a maintenance cycle if you decide to add the iSCSI Fibre Channel zoning members to an effective configuration. Reenabling the effective configuration will affect the entire fabric.

5. Click **OK**.

The effective configuration is modified and reenabled.

MANAGING AND TROUBLESHOOTING ACCESSIBILITY

The Web Tool iSCSI accessibility feature helps you:

- Verify that both host and target are online.
- Verify that the effective discovery domain set has both host and target.
- Allow an initiator or target to access the other.
- Deny an initiator or target to access the other.
- Verify that the iSCSI Fibre Channel zone has been set up and, if appropriate, enable the defined configuration. See [“To create an iSCSI Fibre Channel zone with an effective zone configuration”](#) on page 188

14 Setting up iSCSI Target Gateway Services

Using the Access Gateway

Brocade Access Gateway allows multiple host bus adapters (HBAs) to access the fabric using fewer physical ports. Access Gateway mode transforms the 4012, 4016, 4020, 4024, and 200E into a device management tool that is compatible with different types of fabrics, including Brocade-, Brocade Enterprise OS (EOS), and Cisco-based fabrics.

When a switch is in Access Gateway mode, it is logically transparent to the host and the fabric. Brocade Access Gateway mode allows hosts to access the fabric without increasing the number of switches and simplifies configuration and management in a large fabric by reducing the number of domain IDs and ports.

Brocade Access Gateway is a device management tool and provides only a subset of Fabric OS commands. It does not consume critical fabric elements that could inhibit scalability. For example, a fabric that uses Access Gateways to connect hosts requires fewer domain IDs.

For detailed descriptions of the Access Gateway, see *Brocade Access Gateway Administrator's Guide*.

NOTE

When Access Gateway mode is enabled on switches managed through Web Tools, only a limited subset of menus and options related to device management are available. A switch in Access Gateway mode is considered a device management tool and not a fabric switch, therefore all fabric related options are disabled.

Enabling Access Gateway mode

Once you enable Access Gateway mode, only a limited subset of switch menus are available; fabric management menus are grayed out. All fabric-related service requests are forwarded to the fabric switches.

When you enable Access Gateway mode some fabric information is erased, such as the zone and security databases. To recover the information save the switch configuration before enabling Access Gateway mode.

To save the switch configuration using Web Tools, go to the **Configure > Upload/Download** subtab and upload the configuration file.

To enable Access Gateway mode

1. Select a switch.
2. Click **Switch Admin** in the **Manage** section under **Tasks**.
The Switch Administration window opens.
3. Save the switch configuration.
4. On the **Switch** tab, click the **Disable** radio button in the **Switch Status** section.

15 Displaying the port mapping

5. Click the **Enable** radio button in the **Access Gateway Mode** section.
6. Click **Apply**.
7. Click **Yes** to restart the switch in Access Gateway mode.

To disable Access Gateway mode

1. Select a switch.
2. Click **Switch Admin** in the **Manage** section under **Tasks**.
The Switch Administration window opens.
3. Save the switch configuration.
4. On the **Switch** tab, click the **Disable** radio button in the **Switch Status** section.
5. Click the **Disable** radio button in the **Access Gateway Mode** section.
6. Click **Apply**.
7. Click **Yes** to restart the device in native switch mode.

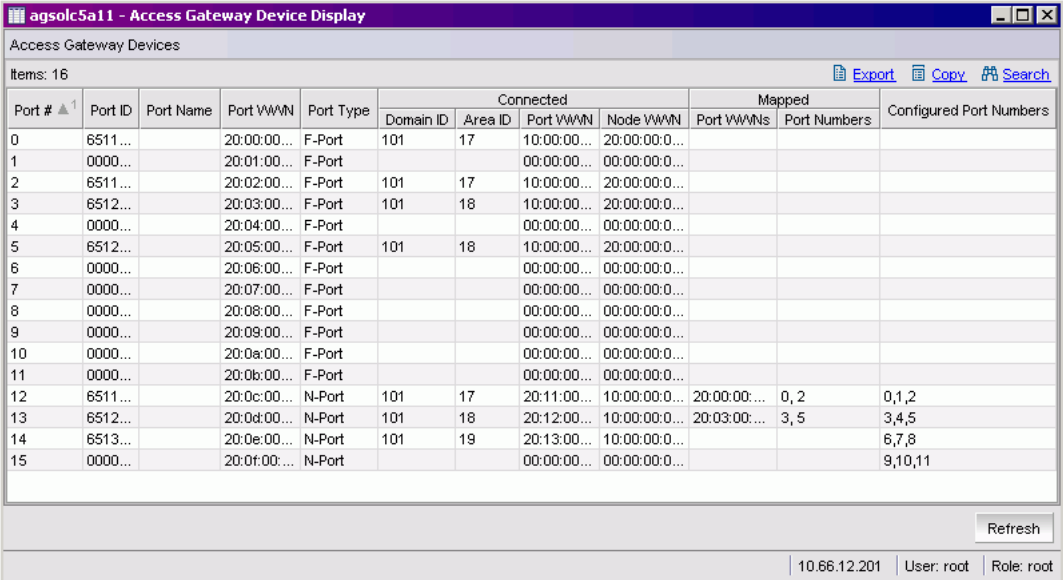
Displaying the port mapping

This section explains how to display the mapped routes of the host connections (F-ports) to the fabric (N-ports) on Brocade Access Gateway. F_Ports are mapped to N_Ports.

To display port mapping

1. Click Access Gateway Devices in the **Monitor** section under **Tasks**.

The Access Gateway Device Display window opens.



Port #	Port ID	Port Name	Port WWN	Port Type	Connected				Mapped		Configured Port Numbers
					Domain ID	Area ID	Port WWN	Node WWN	Port WWNs	Port Numbers	
0	6511...		20:00:00...	F-Port	101	17	10:00:00...	20:00:00:0...			
1	0000...		20:01:00...	F-Port			00:00:00...	00:00:00:0...			
2	6511...		20:02:00...	F-Port	101	17	10:00:00...	20:00:00:0...			
3	6512...		20:03:00...	F-Port	101	18	10:00:00...	20:00:00:0...			
4	0000...		20:04:00...	F-Port			00:00:00...	00:00:00:0...			
5	6512...		20:05:00...	F-Port	101	18	10:00:00...	20:00:00:0...			
6	0000...		20:06:00...	F-Port			00:00:00...	00:00:00:0...			
7	0000...		20:07:00...	F-Port			00:00:00...	00:00:00:0...			
8	0000...		20:08:00...	F-Port			00:00:00...	00:00:00:0...			
9	0000...		20:09:00...	F-Port			00:00:00...	00:00:00:0...			
10	0000...		20:0a:00...	F-Port			00:00:00...	00:00:00:0...			
11	0000...		20:0b:00...	F-Port			00:00:00...	00:00:00:0...			
12	6511...		20:0c:00...	N-Port	101	17	20:11:00...	10:00:00:0...	20:00:00:...	0, 2	0,1,2
13	6512...		20:0d:00...	N-Port	101	18	20:12:00...	10:00:00:0...	20:03:00:...	3, 5	3,4,5
14	6513...		20:0e:00...	N-Port	101	19	20:13:00...	10:00:00:0...			6,7,8
15	0000...		20:0f:00...	N-Port			00:00:00...	00:00:00:0...			9,10,11

FIGURE 89 Access Gateway Device Display

Configuring port maps

To configure a port map

1. Click a port in the Switch View to open the Port Administration window.
2. Click the **FC Ports** tab.
3. Click the **Edit Configuration** button.
4. Click **Save**.

Enabling failover and failback policies

The failover and failback policies determine the behavior of the F_Port if the N_Port they are mapped to goes OFFLINE or is disabled. By default, the failover and failback policies are enabled.

A switch in Access Gateway mode supports automatic N_Port failover to other N_Ports connected to the same fabric. When a port is first configured as an N_Port, the failover policy is enabled by default. If the N_Port goes offline, the F_Ports mapped to that N_Port are automatically failed over to other online N_Ports connected to the same fabric. If there are multiple online N_Ports connected to the same fabric, the mapped F_Ports are distributed evenly between the N_Ports. Failover generates an error message.

A switch in Access Gateway mode supports automatic F_Port failback to N_Ports when that port comes back online. By default the failback policy is enabled. When an N_Port with an enabled failback policy comes back online, the F_Ports that were originally mapped to it are automatically rerouted back to the N_Port.

To enable N Port failover policies

1. Click a port in the Switch View to open the Port Administration window.
2. Click the **FC Ports** tab.
3. Click the **Edit Configuration** button.
4. In the N Port Configuration window, select the **Enable N Port Failover Policy** radio button.
5. Click **Save**.

To enable N Port failback policies

1. Click a port in the Switch View to open the Port Administration window.
2. Click the **FC Ports** tab.
3. Click the **Edit Configuration** button.
4. In the N Port Configuration window, select the **Enable N Port Failback Policy** radio button.
This option is available only if you've selected the **Enable N Port Failover Policy** radio button.
5. Click **Save**.

Converting ports

To convert an F-port to an N-port

1. Click a port in the Switch View to open the Port Administration window.
2. Select the F-port you want to map.

If the F-port is mapped to an N-port, you must unmap it by selecting the mapped N-port and clicking the **Edit Configuration** button. Select the F-port you want to unmap, click Remove, and then click Save.

3. Click the **Edit Configuration** button.

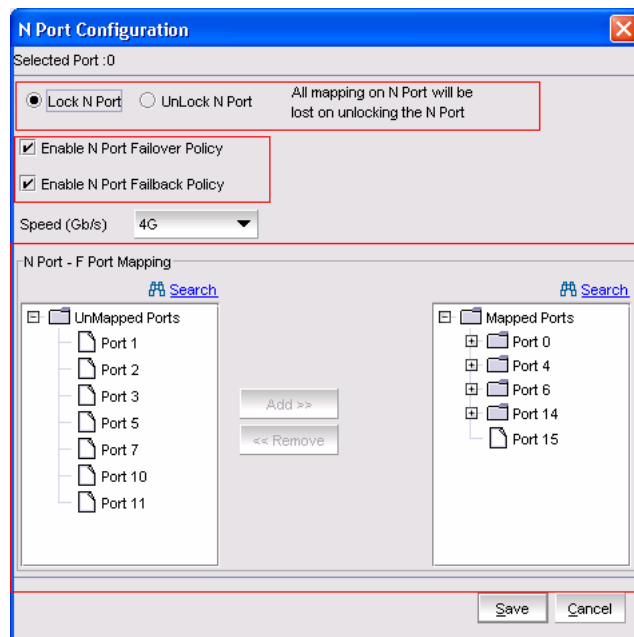


FIGURE 90 N Port Configuration dialog box

4. Select the **Lock N Port** radio button.
5. Select the appropriate failback and failover policies.
6. In the N Port - F Port Mapping area, select the F-port you want to map from the UnMapped Ports list, and click the **Add** button.
7. Click **Save**.

To convert an N-port to an F-port

When you convert an N-port to an F-port, any F-ports mapped to the N-port become unmapped. Traffic is interrupted and the ports will be offline until they are manually mapped to an N-port.

NOTE

To prevent traffic interruption, it is recommended that you reassign any F-ports mapped to the N-port you are converting before you convert the N-port.

1. Click a port in the Switch View to open the Port Administration window.
2. Select the N-port you want to convert to an F-port.

If the N-port has F-ports mapped to it, unmap the F-ports by selecting the mapped N-port and clicking the **Edit Configuration** button. Select the F-port you want to unmap, click Remove, and then click Save. When you have removed all the F-ports, click **Save**.

3. Click the **Edit Configuration** button.
4. Select the **UnLock N Port** radio button.
5. Click **Save**.

Map the newly-created F-port to an existing N-port.

Routing Traffic

In this chapter

This chapter contains the following information:

- [“About routing,”](#) next
- [“Displaying FSPF routing”](#) on page 198
- [“Enabling and disabling dynamic load sharing”](#) on page 199
- [“Specifying frame order delivery”](#) on page 199
- [“Configuring link cost”](#) on page 200

About routing

For Fabric OS 5.2.0, the supported routing policies are:

- Port-based routing
Port-based routing assigns a “static route,” in which the path chosen for traffic never changes.
- Exchanged-based routing (Brocade 4100, 5000, and 48000 only).
Exchange-based routing policy is the default. Exchange-based routing policy always employs “dynamic path selection,” in which the software chooses a path based on current traffic conditions.

See the *Fabric OS Administrator’s Guide* for more information.

To optimize port-based routing, the dynamic load sharing feature (DLS) can be enabled to balance the load across the available output ports within a domain. Exchange-based routing *requires* the use of DLS; when this policy is in effect, you cannot disable the DLS feature.

To configure routing policies, you must use the command line interface (CLI). After the routing policies are configured, you can use Web Tools to display the routing paths and configure routing parameters, such as DLS, frame order delivery, and link cost.

The Routing tab of the Switch Administration window displays routing information. [Figure 91](#) on page 198 shows a Routing tab when the port-based routing policy is enabled. When an exchange-based routing policy is enabled, the Dynamic Load Sharing radio buttons are not displayed.

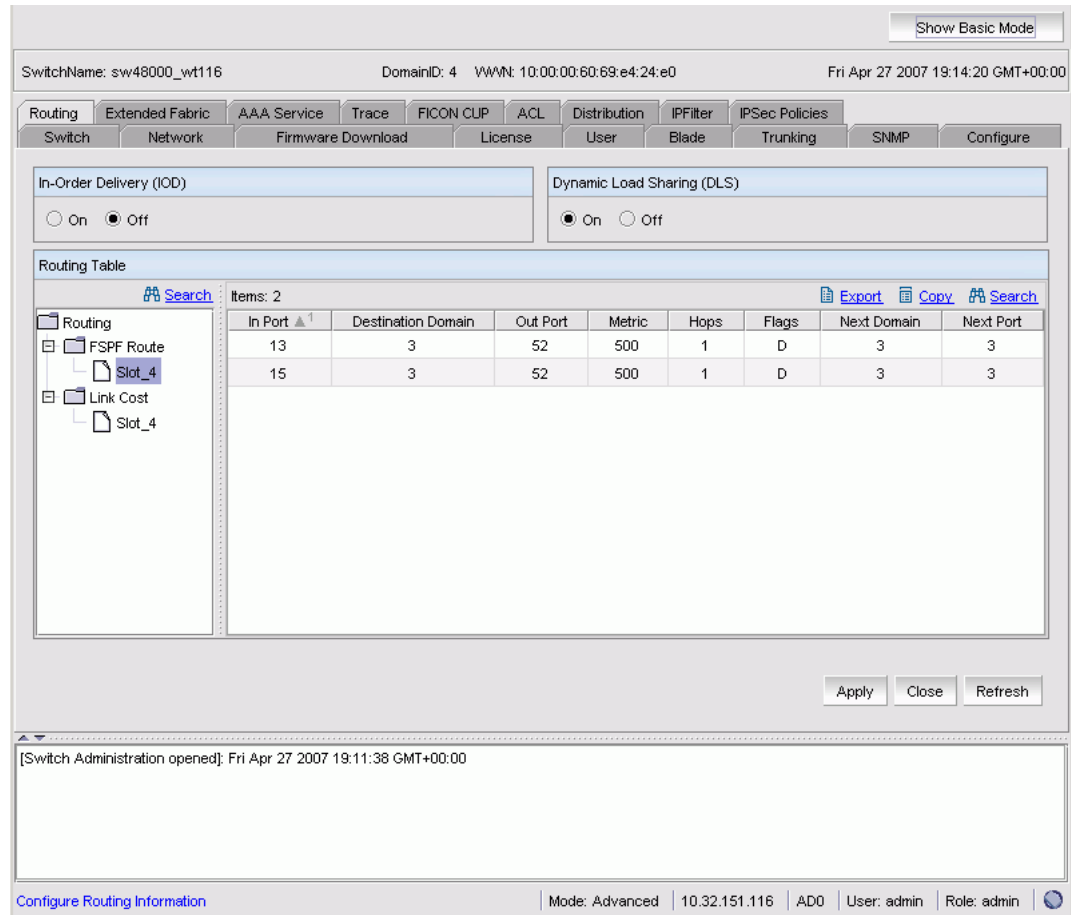


FIGURE 91 Routing tab for port-based routing policy

Displaying FSPF routing

The **Routing** tab of the Switch Administration window displays information about routing paths.

To view FSPF routing

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **Routing** tab.
3. This step is switch-type specific:

For Brocade 24000 or 48000 directors, click a slot number under the FSPF Route category in the navigation tree.

For Brocade 200E, 3250, 3850, 3900, 4012, 4016, 4018, 4020, 4024, 4100, 4900, 5000, and 7500 switches, click the FSPF Route category in the navigation tree.

Enabling and disabling dynamic load sharing

The exchange-based routing policy depends on the Fabric OS dynamic load sharing feature (DLS) for dynamic routing path selection. When this policy is in force, DLS is always enabled and cannot be disabled.

When the port-based policy is in force, you can enable DLS to optimize routing. When DLS is enabled, it shares traffic among multiple equivalent paths between switches. DLS recomputes load sharing either when a switch boots up or each time an E_Port or Fx_Port goes online or offline. Enabling this feature allows a path to be discovered automatically by the FSPF path-selection protocol.

For more information regarding DLS, see the **disset** command in the *Fabric OS Command Reference*.

When you enable or disable dynamic load sharing for a Brocade 24000 or 48000 configured for two logical switches, it is on a logical-switch basis. This means that for each logical switch, you must enable or disable dynamic load sharing individually.

To configure the DLS setting

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **Routing** tab.
3. Click **On** in the Dynamic Load Sharing (DLS) area to enable dynamic load sharing or click **Off** to disable dynamic load sharing.

When the exchange-based routing policy is in effect, the DLS radio buttons do not display in the **Routing** tab

4. Click **Apply**.

Specifying frame order delivery

In a stable fabric, frames are always delivered in order, even when the traffic between switches is shared among multiple paths. However, when topology changes occur in the fabric (for example, if a link goes down), traffic is rerouted around the failure, and some frames could be delivered out of order.

By default, frame delivery is out-of-order across topology changes. However, if the fabric contains destination devices that do not support out-of-order delivery, you can force in-order frame delivery across topology changes.

Enabling in-order delivery (IOD) guarantees that frames are either delivered in order or dropped. For more information regarding IOD, see the *Fabric OS Administrator's Guide*.

When you enable or disable IOD for a Brocade 24000 that is configured for two logical switches, it is on a logical-switch basis. This means that for each logical switch, you enable or disable IOD individually.

NOTE

Enabling in-order delivery can cause a delay in the establishment of a new path when a topology change occurs, and therefore should be used with care.

To configure the IOD setting

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **Routing** tab.
3. Click **On** in the In-Order Delivery (IOD) area to force in-order frame delivery across topology changes or click **Off** to restore out-of-order frame delivery across topology changes.
4. Click **Apply**.

Configuring link cost

This section describes how to set the cost of an interswitch link (ISL). The cost of a link is a dimensionless positive number. The fabric shortest path first (FSPF) protocol compares the cost of various paths between a source switch and a destination switch by adding the costs of all the ISLs along each path. FSPF chooses the path with minimum cost. If multiple paths exist with the same minimum cost, FSPF employs load sharing over these paths.

Every ISL has a default cost that is inversely proportional to its bandwidth. For a 1-Gbit/sec ISL, the default cost is 1000. For a 2-Gbit/sec ISL, the default cost is 500.

Use this procedure to set a non-default, “static” cost for any port.

When you configure link cost for a Brocade 24000 or 48000 configured for two logical switches, it is on a logical-switch basis. This means that for each logical switch, you configure link cost individually.

To configure the link cost for a port

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **Routing** tab.
3. This step is switch-specific:

For Brocade 24000 and 48000 directors, click the slot number of the logical switch under **Link Cost** in the navigation tree.

For Brocade 200E, 3250, 3850, 3900, 4012, 4016, 4018, 4020, 4024, 4100, 4900, 5000, and 7500 switches, click **Link Cost** in the navigation tree.

4. Double-click in the row in the **Cost** column that corresponds to the appropriate port.
5. Type the link cost.

Valid values for link cost are from 1 through 65535. Setting the value to 0 sets the link cost to the default value for that port.

6. Click **Apply**.

Configuring Standard Security Features

In this chapter

This chapter contains the following information:

- [Creating and maintaining user-defined accounts . 201](#)
- [Configuring access control list policies 209](#)
- [Configuring SNMP 211](#)
- [Managing RADIUS service 213](#)

Creating and maintaining user-defined accounts

In addition to the default accounts—root, factory, admin, and user—Fabric OS supports up to 256 user-defined accounts in each logical switch (domain). These accounts expand your ability to track account access and audit administrative activities.

Each user-defined account is associated with the following:

- Admin Domain list—Specifies what Admin Domains a user account is allowed to log in to.
- Home Admin Domain—Specified the Admin Domain that the user is logged in to by default. The home Admin Domain must be a member of the user's Admin Domain list.
- Role—Determines functional access levels within the bounds of the user's current Admin Domain.

Access rights for any user session are determined both by the user's role-based access rights and by the contents of the currently selected Admin Domain. See [Chapter 1, "Introducing Web Tools"](#) for additional information about Admin Domains and Role-Based Access Control (RBAC).

The **User** tab of the Switch Administration window (see [Figure 92](#) on page 203) displays account information. You can create and manage accounts depending on your role:

TABLE 12 User role and permissions

Role	Permissions
admin	Create and manage all predefined and user-defined accounts
operator	Change your own password and cannot create, modify, or view predefined or user-defined accounts
securityadmin	Create and manage all security roles.
switchadmin	Change your own password and cannot create, modify, or view predefined or user-defined accounts
zoneadmin	Change your own password and cannot create, modify, or view predefined or user-defined accounts
fabricadmin	Change your own password and cannot create, modify, or view predefined or user-defined accounts
basicswitchadmin	Change your own password and cannot create, modify, or view predefined or user-defined accounts
user	Change your own password and cannot create, modify, or view predefined or user-defined accounts

NOTE

If you are operating in secure mode, you can perform these operations only on the primary FCS switch.

For legacy users with no Admin Domain specified, the user will have access to AD 0 through 255 (physical fabric admin) if their current role is Admin; otherwise, the user will have access to ADO only.

If some Admin Domains have been defined for the user and all of them are inactive, the user will not be allowed to log in to any switch in the fabric.

If no Home Domain is specified for a user, the system provides a default home domain. The default home domain for predefined account is ADO. User-defined accounts, the default home domain is the Admin Domain in the user's Admin Domain list with the lowest ID.

NOTE

The **User** tab displays and changes information in the switch database. If you have RADIUS configured, note that this tab displays the logged-in RADIUS account information but does not allow the user to modify the RADIUS host server database.

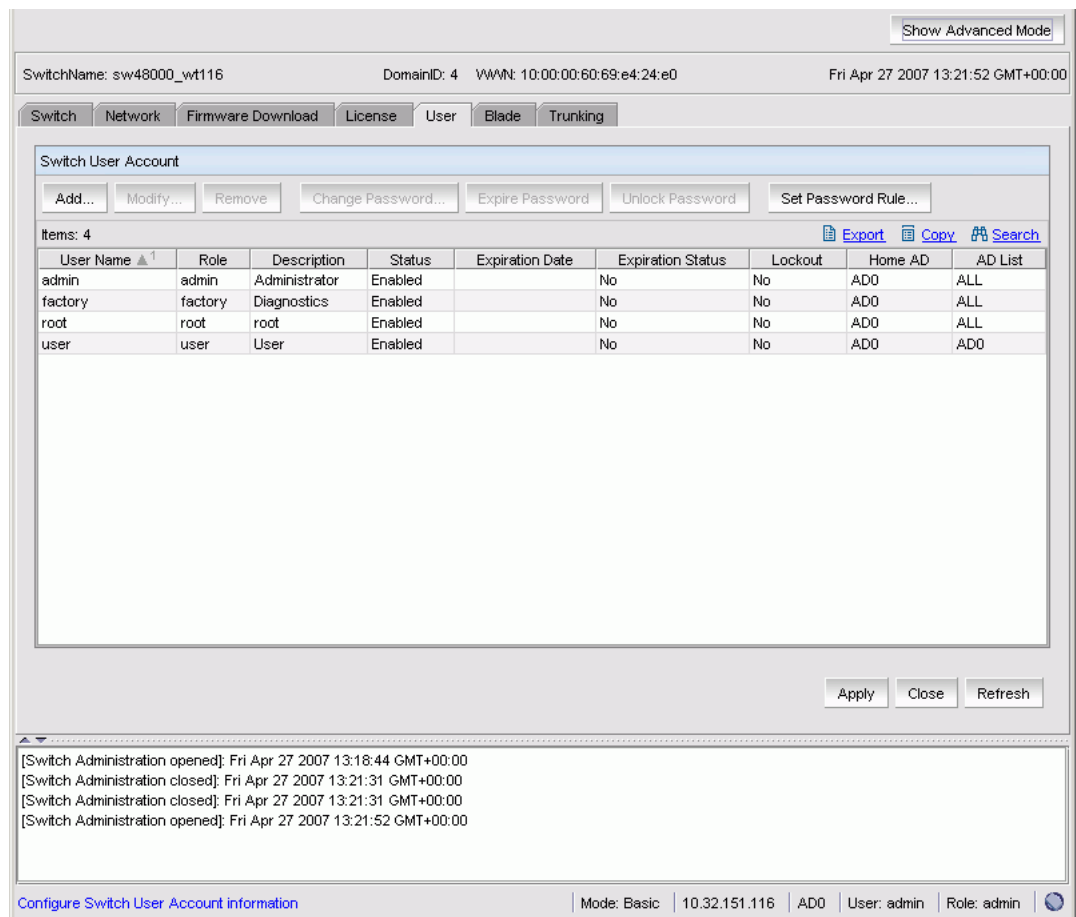


FIGURE 92 User tab

To display account information

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **User** tab.

A list of the default and user-defined accounts appears. If you are logged in using the switchadmin role, only your account information is displayed.

CREATING AND DELETING USER-DEFINED ACCOUNTS

This section describes how to create and delete user-defined accounts.

To create a user-defined account

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **User** tab.
3. Click **Add**.

The Add User Account dialog box opens.

FIGURE 93 Add User Account dialog box

4. Type the user name, which must begin with an alphabetic character. The name can be up to 40 characters long. It is case-sensitive and can contain alphabetic and numeric characters, the dot (.) and the underscore (_). It must be different from all other account names on the logical switch.
5. Select a role from the drop-down menu. (See [“Role-Based access control”](#) on page 11 for information about these roles.)
6. *Optional:* Type a description of the account.
7. Click the **Enabled** or **Disabled** radio button to enable or disable the account.
8. Type the password for the account. The password is not displayed when you enter it on the command line.

Passwords can be from 8 through 40 characters long. They must begin with an alphabetic or numeric character. They can include alphanumeric characters, the dot (.), and the underscore (_). They are case-sensitive.

Passwords must also meet any additional password rules that have been set up. (See the procedure [“To set the rules for passwords”](#) on page 207 for more information.)

9. Retype the password in the **Confirm Password** field for confirmation.
10. Check the available Admin Domains that the user can access. Only Admin Domains that have already been created and to which you have access are displayed.

If all the Admin Domains in the list are inactive then you cannot login to the switch.

The **All** option does not mean all of the listed Admin Domains; it means all Admin Domains from ADO through AD255, regardless of whether they have been created yet.

The **All** radio button is disabled unless the following conditions are met:

- The selected role for the target user must be admin or securityadmin.
- You must be a physical fabric administrator.

Selecting **All** makes the target user account a physical fabric administrator.

11. Select a home domain for the user from the Home AD drop-down menu.

If ADO is deselected in the user's Admin Domain list and no other Admin Domains have been selected, the next available Admin Domain becomes the user's default home Admin Domain.

12. Click **OK**.

13. On the **User** tab, click **Apply** to apply your changes.

To delete a user-defined account

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **User** tab.
3. Select the account to remove and click **Remove**.
4. Click **Apply** to save your changes.

You cannot delete the default accounts. An account cannot delete itself. All active command line interface (CLI) sessions for the deleted account are logged out.

CHANGING ACCOUNT PARAMETERS

Use the following procedure to change the role, add or change the description, and enable or disable accounts. Note that you cannot change the user name of the account using this procedure. To change the user name, you must delete the account and create a new account.

Users can select their own accounts in the user account table and change the password. All other buttons will be unavailable.

To change account parameters

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **User** tab.
3. Select the account to modify.

You cannot modify the default root and factory accounts, even if you are logged in as root.

4. Click the **Modify** button.

If the user account you are modifying doesn't have a subset of your Admin Domains, a warning message is displayed to inform you of the permissions conflict.

The Modify User Account dialog box displays.

5. Select a role from the drop-down menu.

You can change the role only on user-level accounts. You cannot change the role on the admin or root accounts. You cannot change the role of your own account.

6. Type a new description.

You can change the description only on user-level accounts. You cannot change the description of the default accounts. You cannot change the description of your own account.

7. Click the **Enabled** or **Disabled** radio button to enable or disable the account.

You can enable and disable user- and admin-level accounts except for your own account. You cannot enable or disable your own account or the factory account. Only the root account can disable itself. If you disable an account, all active CLI sessions for that account are logged out.

8. Check the available Admin Domains that the user can access. Only Admin Domains that have already been created and to which you have access are displayed.

If all the Admin Domains in the list are inactive then you can't login to the switch.

The **All** option does not mean all of the listed Admin Domains; it means all Admin Domains from ADO through AD255, regardless of whether they have been created yet.

The **All** radio button is disabled unless the following conditions are met:

- The selected role for the target user must be admin or securityadmin.
- You must be a physical fabric administrator.

Selecting **All** makes the target user account a physical fabric administrator.

9. Select a home domain for the user from the Home AD drop-down menu.

If ADO is deselected in the user's Admin Domain list and no other Admin Domains have been selected, the next available Admin Domain becomes the user's default home Admin Domain.

10. Click **OK** and click **Apply** to apply your changes.

MAINTAINING PASSWORDS

This section contains procedures for the following:

- [To change account parameters](#) 205
- [To set the rules for passwords](#) 207
- [To expire a password](#) 208
- [To unlock a password](#) 208

When you expire a password, the next time that user logs in, Web Tools requires the user to provide a new password.

NOTE

You have to own the switch in order to modify password rules.

A password becomes locked if a user has exceeded the maximum number of failed login attempts. This number is specified in the **Lockout Threshold** field shown in [Figure 94](#). To unlock a locked password, see the unlock procedure on [page 208](#).

To change the password of an account

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **User** tab.
3. Select the account to modify.

If you are logged in as admin, you can change the password of your own account, peer admin accounts, switchadmin accounts, and user accounts. You can also change the root or factory account passwords.

If you are logged in as a switchadmin, you can only change the password of your own account.

4. Click **Change Password**.

The Set User Account Password dialog box displays.

If you are changing the password of an admin account, you must also provide the current password. You do not need to provide the current password if you are changing the password of a lower-level user account.

5. Type the current password of the account. This step is required only if you are changing the password of your own or a peer admin account.

6. Type the new password of the account.

The new password must have at least one character different from the old password.

Passwords can be from 8 through 40 characters long. They must begin with an alphabetic or numeric character. They can include alphanumeric characters, the dot (.), and the underscore (_). They are case-sensitive.

Passwords must also meet any additional password rules that have been set up. (See the procedure [“To set the rules for passwords”](#) on page 207 for more information.)

7. Retype the new password in the **Confirm Password** field.

8. Click **OK**.

9. Click **Apply** to save your changes.

To set the rules for passwords

1. Open the Switch Administration window as described on [page 31](#).

2. Click the **User** tab.

3. Click **Set Password Rule**.

The Configure Password Rule dialog box displays, as shown in [Figure 94](#) on page 208.

4. Fill out the dialog box for the password rules you want to enforce. Options are:

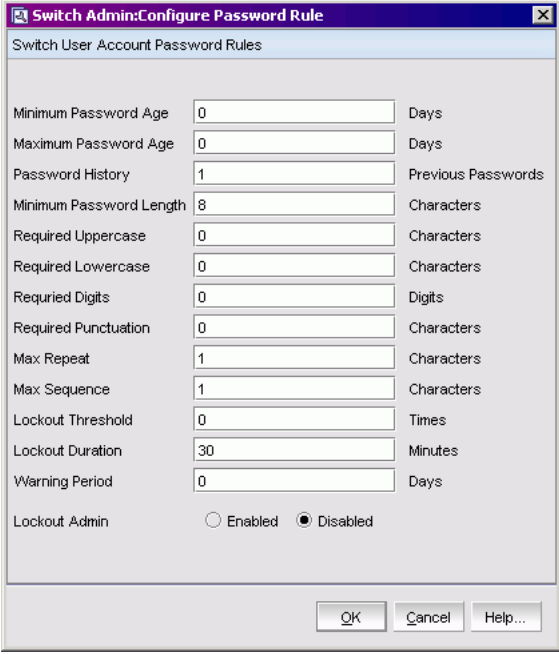
- Minimum number of days (0–999) before you can change the password again
- Number of days (0–999) before a password expires
- Number of password changes before you can reuse a password
- Minimum password length (8–40 characters)
- Minimum number of uppercase and lowercase characters required
- Minimum number of digits and punctuation characters required
- Number of characters that can be repeated in the password
- Number of failed login attempts (0–999) before the password is locked from further change attempts, and the amount of time the password will be locked (0–99999 minutes)
- Number of days to warn user before password expiration (0–999)

5. Choose whether to enable or disable the lockout administration features.

If you choose to disable the lockout administration, the user is never locked out of the system.

17 Creating and maintaining user-defined accounts

6. Click **OK** to close the dialog box.
7. Click **Apply** to save your changes.



The image shows a Windows-style dialog box titled "Switch Admin: Configure Password Rule". The main area is labeled "Switch User Account Password Rules". It contains several configuration options, each with a text input field and a unit label to its right:

- Minimum Password Age: 0 Days
- Maximum Password Age: 0 Days
- Password History: 1 Previous Passwords
- Minimum Password Length: 8 Characters
- Required Uppercase: 0 Characters
- Required Lowercase: 0 Characters
- Required Digits: 0 Digits
- Required Punctuation: 0 Characters
- Max Repeat: 1 Characters
- Max Sequence: 1 Characters
- Lockout Threshold: 0 Times
- Lockout Duration: 30 Minutes
- Warning Period: 0 Days

At the bottom left, there is a "Lockout Admin" section with two radio buttons: "Enabled" (which is unselected) and "Disabled" (which is selected).

At the bottom right, there are three buttons: "OK", "Cancel", and "Help...".

FIGURE 94 Configure Password Rules dialog box

To expire a password

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **User** tab.
3. Select the account.
4. Click **Expire Password**.

If the button is unavailable, this means the password is already expired.

5. Click **Apply** to save your changes.

To unlock a password

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **User** tab.
3. Select the account.
4. Click **Unlock Password**.

If the button is unavailable, this means the password is already unlocked or was not locked out.

5. Click **Apply** to save your changes.

Configuring access control list policies

Support for the Access Control List (ACL) policies is currently defined in the Switch Connection Control (SCC) and Device Connection Control (DCC) policies. These policies are unlike the Secure Fabric OS policies. In Secure Fabric OS where the SCC and DCC policies are always fabric wide policies, these policies located in the Admin module are switch-based. ACL and Secure Fabric OS are mutually exclusive. Unlike in Secure Fabric OS, SCC and DCC policy configuration in base Fabric OS is performed on a switch-local basis.

Admin Domain considerations: ACL management can be done on AD255 and in AD0 only if other there are no user-defined Admin Domains. Both AD0 (when no other user-defined Admin Domains exist) and AD255 provide an unfiltered view of the fabric.

SwitchName: sw48000_wt116 DomainID: 4 WWN: 10:00:00:60:69:e4:24:e0 Fri Apr 27 2007 13:31:56 GMT+00:00

Routing Extended Fabric AAA Service Trace FICON CUP ACL Distribution IPFilter IPsec Policies
Switch Network Firmware Download License User Blade Trunking SNMP Configure

ACL - Switch Connection Control Policy

Accept Distribution

General Information
Accepts Distribution No
Policy Scope Absent

Members of SCC Policy

Defined Policy Set Search

Active Policy Set Search

SCC DCC

Edit Activate Close Refresh

[Switch Administration opened]: Fri Apr 27 2007 13:16:44 GMT+00:00
[Switch Administration closed]: Fri Apr 27 2007 13:21:31 GMT+00:00
[Switch Administration closed]: Fri Apr 27 2007 13:21:31 GMT+00:00
[Switch Administration opened]: Fri Apr 27 2007 13:21:52 GMT+00:00

ACL Admin Panel Mode: Advanced 10.32.151.116 AD0 User: admin Role: admin

FIGURE 95 ACL tab for SCC/DCC policy configuration

To create an SCC or DCC policy

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **ACL** tab.
3. Select an SCC or DCC policy by clicking on the appropriate tab.
4. Click **Edit**.

This launches the ACL Policy Configuration wizard.

5. Select the policy type you want to edit.
6. Click **Next** and click **Create**.
7. *DCC Option:* Select a switch or highlight multiple switches to add to an DCC policy by clicking **Add** or **Add All**.

To add an offline switch, click **Add other Switch** and enter the WWN.

8. *SCC Option:* Select the ports to add to an DCC policy by clicking **Add** or **Add All**.
9. Click **Finish** to confirm the changes to the switch.

You must activate the policy in order to implement it. See [“To activate an SCC or DCC policy”](#) on page 210, for instructions.

To edit an SCC or DCC policy

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **ACL** tab.
3. Select a SCC or DCC policy by clicking on the appropriate tab.
4. Click **Edit**.

This launches the ACL Policy Configuration wizard.

5. Select the policy type you want to edit.
6. Click **Next** and click **Modify**.
7. Select a switch or highlight multiple switches to add to the policy by clicking **Add** or **Add All**.
8. Click **Next** and click **Finish** to confirm the changes to the switch.

To delete an SCC/DCC policy

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **ACL** tab.
3. Select a SCC or DCC policy by clicking on the appropriate tab.
4. Click **Edit**.

This launches the ACL Policy Configuration Wizard.

5. Select the policy type you want to edit.
 6. Click **Next** and click **Delete**.
- When members are present then the “Delete” button is displayed.
7. Click **Next** and click **Finish** to confirm the changes to the switch.

To activate an SCC or DCC policy

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **ACL** tab.
3. Select a SCC or DCC policy by clicking on the appropriate tab.
4. Click **Activate**.

Activating the policy moves it into the Activate Policy Set window.

Once a SCC/DCC policy has been created or modified you can distribute it to the rest of the fabric:
To deactivate an SCC or DCC policy, you must activate a new or empty policy.

To distribute an SCC or DCC Policy

1. Open the Switch Administration window as described on [page 31](#).
2. Select the **Distribution** tab
3. Select the appropriate behavior from the **Consistency Behavior** drop-down menu:
 - Absent means that there will be no policy pushed out to other switches
 - Tolerant means that the policy will allow legacy switches
 - Strict means that only Fabric OS version 5.2.0 and above switches are allowed
4. Select **Apply**

If the policy distribution fails, an error dialog box is displayed.

Configuring SNMP

This section describes how to manage the configuration of the SNMP agent in the switch. The configuration includes SNMPv1 and SNMPv3 configuration, accessControl, and systemGroup configuration parameters.

NOTE

This module is read-only if you do not own the switch.

For more information, see the **snmpConfig** command in the *Fabric OS Command Reference*.

SETTING SNMP TRAP LEVELS

When you set trap levels for a Brocade 24000 or 48000 configured with two logical switches, it is on a logical-switch basis. This means that for each logical switch, you must set trap levels individually.

To set trap levels

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **SNMP** tab.

SwitchName: sw48000_wt116 DomainID: 1 VVWV: 10:00:00:60:69:e4:24:e0 Thu Apr 26 2007 15:33:41 GMT+00:00

Routing Extended Fabric AAA Service Trace FICON CUP ACL Distribution IPFilter IPsec Policies
Switch Network Firmware Download License User Blade Trunking **SNMP** Configure

SNMP Information

Contact Name: Field Support.
Description: Fibre Channel Switch.
Location: End User Premise.

Enable/Disable Authentication Trap
☐ Enable Authentication Trap

SNMPv3 Trap Recipient

Items: 6 [Export](#) [Copy](#) [Search](#)

User Name ▲	Recipient IP	Trap Level
snmpadmin1 - RW	0.0.0.0	0 - None
snmpadmin2 - RW	0.0.0.0	0 - None
snmpadmin3 - RW	0.0.0.0	0 - None

SNMPv1 Community/Trap Recipient

Items: 6 [Export](#) [Copy](#) [Search](#)

Community String	Recipient	Access Control	Trap Level
Secret C0de	0.0.0.0	Read Write	0 - None
OrigEquipMfr	0.0.0.0	Read Write	0 - None
private	0.0.0.0	Read Write	0 - None

Access Control List

Apply Close Refresh

[Switch Administration opened]: Thu Apr 26 2007 14:14:19 GMT+00:00

Configure SNMP parameters Mode: Advanced 10.32.151.116 AD0 User: admin Role: admin

FIGURE 96 SNMP tab

3. Select a trap level for a recipient from the corresponding **Trap Level** drop-down menu in the SNMPv1 and SNMPv3 sections.

The level you select identifies the minimum event level that will prompt a trap.

4. Click **Apply**.

CONFIGURING SNMP INFORMATION

When you configure SNMP information for a Brocade 24000 or 48000 configured with two logical switches, it is on a logical-switch basis. This means that for each logical switch, you must configure SNMP information individually.

To change the systemGroup configuration parameters

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **SNMP** tab (see [Figure 96](#)).

3. Type a contact name, description, and location in the **SNMP Information** section.
4. *Optional:* Select the **Enable Authentication Trap** check box to allow authentication traps to be sent to the reception IP address.
5. Click **Apply**.

To set SNMPv1 configuration parameters

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **SNMP** tab (see [Figure 96](#)).
3. Double-click a community string in the **SNMPv1** section and type a new community string.
4. Double-click a recipient IP address in the **SNMPv1** section and type a new IP address.
5. Click **Apply**.

To set SNMPv3 configuration parameters

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **SNMP** tab (see [Figure 96](#)).
3. Select a user name from the User Name drop-down menu in the **SNMPv3** section.
Note that the list is scrollable. If you do not see your user name, scroll down using the scroll bar or by clicking the User Name heading.
4. Double-click a recipient IP address in the **SNMPv3** section and type a new IP address.
5. Select a trap level from the **Trap Level** drop-down menu.
6. Click **Apply**.

To change the access control configuration

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **SNMP** tab (see [Figure 96](#)).
3. Double-click an access host IP address in the **Access Control List** section and type a new host IP address.
Note that the list is scrollable. If you do not see your user name, scroll down using the scroll bar or by clicking the Access Host heading.
4. Select a permission for the host from the **Access Control List** drop-down menu. Options are **Read Only** and **Read Write**.
5. Click **Apply**.

Managing RADIUS service

Fabric OS supports RADIUS authentication, authorization, and accounting service (AAA). When configured for RADIUS, the switch becomes a Network Access Server (NAS) that acts as a RADIUS client. In this configuration, authentication records are stored in the RADIUS host server database. Login and logout account name, assigned role, and time accounting records are also stored on the RADIUS server.

You should set up RADIUS service through a secure connection such as SSH.

The three choices in the drop-down menu when RADIUS is selected as the primary service are:

- **Switch Database when RADIUS Authentication Fails**—When selected, the switch user login database will be checked whenever RADIUS authentication fails.
- **Switch Database When RADIUS Times Out**—Switch user login database is checked only if the physical connection to the RADIUS server fails.
- **None**—Switch user login database is never checked. Only a RADIUS server can be used for authentication.

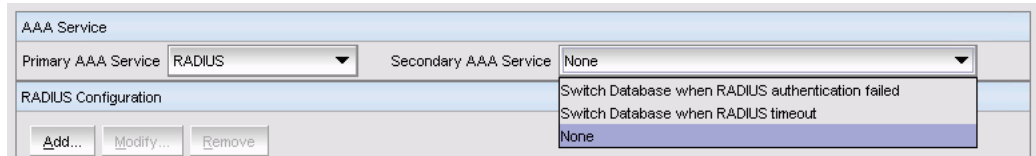


FIGURE 97 Choices in the Secondary AAA Service drop-down menu

If the switch database is selected as primary, there is no secondary option. The RADIUS server cannot be configured as a backup for the switch user login database.

When the primary AAA service is RADIUS you can enable the secondary service which offers three choices:

- **None**
- **Switch Database when RADUIS authorization fails**
- **Switch Database when RADIUS times out**

When RADIUS login fails, even though RADIUS server is available, the additional service allows you the option to use the Switch Database as backup authentication service when the RADIUS server is not available. Alternatively, you can have no secondary AAA service, which means that only the primary service will be used for authentication.

Use the **AAA Service** tab of the Switch Administration window to manage the RADIUS service (see [Figure 98](#)).

SwitchName: sw48000_wt116 DomainID: 1 VVWN: 10:00:00:60:69:e4:24:e0 Thu Apr 26 2007 16:25:14 GMT+00:00

Routing Extended Fabric **AAA Service** Trace FICON CUP ACL Distribution IPFilter IPsec Policies
Switch Network Firmware Download License User Blade Trunking SNMP Configure

AAA Service

Primary AAA Service: Switch Database Secondary AAA Service: None

RADIUS Configuration

Add... Modify... Remove

Items: 2

RADIUS Server	Port	Timeout(s)	Authentication
fec0:60:69bc:59:60:69ff:fee4:9008	1812	3	CHAP
fec0:60:69bc:59:60:69ff:fee4:8008	1812	3	CHAP

Export Copy Search

Apply Close Refresh

[Switch Administration opened]: Thu Apr 26 2007 16:13:07 GMT+00:00

FIGURE 98 AAA Service tab

ENABLING AND DISABLING RADIUS SERVICE

At least one RADIUS server must be configured before you can enable RADIUS service.

To enable or disable RADIUS service

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **AAA Service** tab.
3. To enable RADIUS service, select **RADIUS** from the Primary AAA Service drop-down menu. Select **None**, **Switch Database when RADIUS Login Failed**, or **Switch Database when RADIUS Login Timeout** from the Secondary AAA Service drop-down menu.

To disable RADIUS service, select **Switch Database** from the Primary AAA Service drop-down menu and select **None** from the Secondary AAA Service drop-down menu.

4. Click **Apply**.

CONFIGURING THE RADIUS SERVICE

The configuration is chassis-based, so it applies to all logical switches (domains) on the switch and replicates itself on a standby CP, if one is present. It is saved in a configuration upload, and so it can be applied to other switches in a configuration download. You should configure at least two RADIUS servers so that if one fails, the other will assume service.

You can configure the RADIUS service even if it is disabled. You can configure up to five RADIUS servers. You must be logged in as admin or switchadmin to configure the RADIUS service.

To configure the RADIUS service

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **AAA Service** tab.
3. Click **Add**. You can configure up to five RADIUS servers. If five RADIUS servers are already configured, the **Add** button is disabled.

The RADIUS Configuration dialog box displays.

4. Type the RADIUS server name, which is a valid IP address (in either IPv4 or IPv6 format) or Dynamic Name Server (DNS) string. Each RADIUS server must have a unique IP address or DNS name for the RADIUS server.
5. Type the port number.
6. Type the secret string.
7. Type the timeout time in minutes.
8. Select an authentication protocol from CHAP or PAP. The default value is CHAP, and if you do not change it, CHAP will be the authentication protocol.
9. Click **OK** to return to the **AAA Service** tab.
10. Click **Apply**.

MODIFYING THE RADIUS SERVER

Use the following procedure to change the parameters of a RADIUS Server that is already configured.

To modify the RADIUS Server

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **AAA Service** tab.
3. Click a RADIUS server from the **RADIUS Configuration** list.
4. Click **Modify**.

The RADIUS Configuration dialog box displays.

5. Type new values for the port number, secret string, and timeout time (in minutes).
6. Select an authentication protocol from CHAP or PAP. The default value is CHAP, and if you do not change it, CHAP will be the authentication protocol.
7. Click **OK** to return to the **AAA Service** tab and click **Apply**.

MODIFYING THE RADIUS SERVER ORDER

The RADIUS servers are contacted in the order they are listed, starting from the top of the list and moving to the bottom.

To modify the order in which the RADIUS servers are contacted

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **AAA Service** tab.
3. Click a RADIUS server from the RADIUS Configuration list.
4. Click the up and down arrows to rearrange the order of the RADIUS servers.
5. Click **Apply**.

REMOVING A RADIUS SERVER

Use the following procedure to remove a RADIUS server.

To remove a RADIUS server

1. Open the Switch Administration window as described on [page 31](#).
2. Click the **AAA Service** tab.
3. Click a RADIUS server from the RADIUS Configuration list.
4. Click **Remove**. If there is no RADIUS server configured, the **Remove** button is disabled. You cannot remove the only RADIUS server if the RADIUS service is the primary AAA service.
The RADIUS server is not deleted until you apply the changes from the **AAA Services** tab.
5. Click **Apply** in the **AAA Services** tab.
A confirmation displays, warning you that you are about to remove the selected RADIUS server.
6. Click **Yes** in the confirmation.

Administering FICON CUP Fabrics

In this chapter

This chapter contains the following sections:

- [Enabling port-based routing on the Brocade 4100, 5000, and 48000](#) 220
- [Enabling or disabling FMS mode](#) 221
- [Configuring FMS parameters](#) 222
- [Displaying code page information](#) 223
- [Displaying the control device state](#) 223
- [Configuring CUP port connectivity](#) 224

About FICON CUP fabrics

Control Unit Port (CUP) is a protocol for managing FICON directors. Host-based management programs manage the switches using CUP protocol by sending commands to the emulated control device implemented by Fabric OS. A Brocade switch or director that supports CUP (Brocade 3900, 24000, or 48000) can be controlled by one or more host-based management programs or director consoles, such as Brocade Web Tools or Brocade Fabric Manager. (Refer to the *Fabric Manager Administrator's Guide* for information about Fabric Manager.) The director allows control to be shared between host-based management programs and director consoles.

To use FICON CUP, you must:

- Install a FICON CUP license on a FICON director.
- Enable FMS mode on the FICON director.
- Configure CUP attributes (FMS parameters) for the FICON director.

You can use Web Tools for all of these tasks. You can also use Web Tools to manage FICON directors (when FMS mode is enabled on those directors) to:

- Display the control device state
- Display a code page
- Manage port connectivity configuration

You do not need to install the FICON CUP license to perform FICON CUP management; you *must* install the FICON CUP license, however, if your switch is to enforce traffic between the FICON director and the host-based management program.

Enabling port-based routing on the Brocade 4100, 5000, and 48000

Port-based path selection is a routing policy in which paths are chosen based on ingress port and destination only. This also includes user-configured paths. All Brocade 4100, 5000, and 48000 switches with FICON devices attached must have port-based routing policy enabled. Port-based routing is a per-switch routing policy. After port-based routing is enabled, you can continue with the rest of the FICON implementation.

To enable or disable port-based routing

1. Click a switch with FICON devices attached from the Fabric Tree.
2. Open the Switch Administration window as described on [page 31](#).
3. Click the **FICON CUP** tab.

The FICON CUP tabbed page displays, with the FICON Management Server subtabbed page in front, as shown in [Figure 99](#).

4. Click the **Enable** radio button in the Port Based Routing section to enable the port-based routing policy. Click the **Disable** radio button to disable port-based routing.
5. Click **Apply** to save your changes.

SwitchName: sw48000_wt116 DomainID: 4 VVWN: 10:00:00:60:69:e4:24:e0 Fri Apr 27 2007 19:18:37 GMT+00:00

Routing Extended Fabric AAA Service Trace FICON CUP ACL Distribution IPFilter IPsec Policies
Switch Network Firmware Download License User Blade Trunking SNMP Configure

FICON Management Server Mode
☐ Enable ☒ Disable

FICON Management Server Behavior Control (Mode Register)
☐ Programmed Offline State Control ☐ Director Clock Alert Mode
☐ User Alert Mode ☐ Alternate Control Prohibited
☐ Active=Saved Mode ☐ Host Control Prohibited

Code Page
 Language used to exchange information with Host Programming: 00000

Control Device Allegiance
 Control Device is in unavailable state.

Port Based Routing
☒ Enable (Making change requires disabling switch)

FICON Management Server CUP Port Connectivity

Apply Close Refresh

[Switch Administration opened]: Fri Apr 27 2007 19:11:38 GMT+00:00

Configure FICON CUP Mode: Advanced 10.32.151.116 AD0 User: admin Role: admin

FIGURE 99 FICON CUP management

Enabling or disabling FMS mode

FICON Management Server (FMS) is used to support switch management using CUP. To be able to use the CUP functionality, all switches in the fabric must have FICON Management Server mode (FMS mode) enabled. FMS mode is a per-switch setting. After FMS mode is enabled, you can activate a CUP license without rebooting the director. You can use Web Tools to install a CUP license. For more information on installing licenses, see [“Activating a license on a switch”](#) on page 44.

When FMS mode is disabled, mainframe management applications, director consoles, or alternate managers cannot communicate with a director with CUP. In addition, when FMS mode is disabled on a director, you cannot configure CUP attributes.

To enable or disable FMS mode

1. Click a FICON CUP-capable switch from the [Fabric Tree](#).
2. Open the Switch Administration window as described on [page 31](#).
3. Click the **FICON CUP** tab.

The FICON CUP tabbed page displays, with the FICON Management Server subtabbed page in front, as shown in [Figure 99](#). All attributes on this tab are disabled until FMS mode is enabled.

4. Click the **Enable** radio button in the FICON Management Server Mode section to enable FMS mode or click **Disable** to disable FMS mode.
5. Click **Apply** to save your changes.

Configuring FMS parameters

FMS parameters control the behavior of the switch with respect to CUP itself, as well as the behavior of other management interfaces (director console, Alternate Managers). You can configure FMS parameters for a switch *only* after FMS mode is enabled on the switch. All FMS parameter settings are persistent across switch power cycles. There are six FMS parameters, as described in the table below.

TABLE 13 FMS Mode Parameter Descriptions

Parameter	Description
Programmed Offline State Control	Controls whether host programming is allowed to set the switch offline. The parameter is set as enabled by the hardware after system installation, and can be reset by Web Tools.
Active=Saved Mode	<p>Controls the IPL file update. The IPL file saves port connectivity attributes and port names. After a switch reboot or power cycle, the switch reads the IPL file and activates its contents as default configuration.</p> <p>When this mode is enabled, activating a configuration saves a copy to the IPL configuration file. All changes made to the active connectivity attributes or port names by host programming or alternate managers are saved in this IPL file. It keeps the current active configuration persistent across switch reboots and power cycles.</p> <p>You cannot directly modify the IPL file or save a file as an IPL file. When this mode is disabled, the IPL file is not altered for either new configuration activation or any changes made on the current active configuration. This parameter is set as enabled by the hardware after system installation, and can be reset by Web Tools.</p> <p>Note: When FMS mode is enabled and the Active=Saved parameter is disabled, you can enable and disable ports, but the setting is not persistent. When the Active=Saved parameter is enabled, you can enable and disable ports and the setting is persistent.</p>
Alternate Control Prohibited	<p>Determines whether alternate managers are allowed to modify port connectivity.</p> <p>Enabling this mode prohibits alternate manager control of port connectivity; otherwise, alternate managers can manage port connectivity.</p> <p>This parameter is set as enabled by the hardware after system installation, and can be reset by Web Tools.</p>
User Alert Mode	<p>Controls director console behavior for alerts.</p> <p>Enabling this mode prompts the director consoles to display a warning whenever you attempt an action that will change switch parameters. When you disable this mode, no warning is displayed. In this case, in which Web Tools is the director console, warning messages are displayed by Web Tools regardless of the setting of the parameter, since Web Tools always displays warning messages when you apply a change to a switch that changes parameters. This parameter is always read-only in Web Tools. Each time that the switch is powered on, the parameter is reset to disabled.</p>
Director Clock Alert Mode	<p>Controls behavior for attempts to set the switch timestamp clock through the director console.</p> <p>When it is enabled, the director console (Web Tools, in this case) displays warning indications when the switch timestamp is changed by a user application. When it is disabled, you can activate a function to automatically set the timestamp clock. There is no indication for timestamp clock setting.</p> <p>This parameter is set as disabled by the hardware after system installation, and can be reset by Web Tools.</p>
Host Control Prohibited	<p>Determines whether host programming allows modifying port connectivity.</p> <p>Enabling this mode prohibits host programming control of port connectivity; otherwise, host programming can manage port connectivity.</p> <p>This parameter is set as disabled by the hardware after system installation, and can be reset by Web Tools.</p>

To configure FMS mode parameters

1. Click a FICON-enabled switch from the [Fabric Tree](#).
2. Open the Switch Administration window as described on [page 31](#).
3. Click the **FICON CUP** tab.

The FICON CUP tabbed page displays, with the FICON Management Server subtabbed page in front (see [Figure 99](#) on page 220). All attributes on this tab are read-only until FMS mode is enabled.

4. To enable or disable an FMS mode parameter, click the check box next to the parameter. A marked check box means that the parameter is enabled. You cannot configure the User Alert Mode parameter in Web Tools, as it is read-only.

Displaying code page information

The Code Page field identifies the language used to exchange information between the FICON director and Host Programming. It is a read-only field in Web Tools, as it is set by Host Programming only. When FMS mode is disabled, the code page is displayed as unavailable.

To display the code page information

1. Click a FICON-enabled switch from the [Fabric Tree](#).
2. Open the Switch Administration window as described on [page 31](#).
3. Click the **FICON CUP** tab.

The FICON CUP tabbed page displays, with the FICON Management Server subtabbed page in front (see [Figure 99](#) on page 220). All attributes on this tab are read-only until FMS mode is enabled.

The code page format is displayed in the Code Page field as shown in the example below:

```
Language used to exchange information with Host Programming: (EBCDIC)
USA/Canada -- 00037
```

Displaying the control device state

The control device is in either a neutral or a switched state. When it is neutral, the control device accepts commands from any channel that has established a logic path with it and accepts commands from alternate managers. When the control device is switched, it establishes a logical path and accepts commands only from that logical path (“device allegiance”). Commands from other paths cause a FICON CUP Busy Error. Most “write” operations from alternate managers are also rejected.

Device allegiance usually lasts for a very short time. However, under abnormal conditions, device allegiance can get “stuck” and fail to terminate. It might cause the switch to be unmanageable with CUP, and you will continue to receive the FICON CUP Busy Error. In this case, you should check the control device state and the last update time to identify if the device allegiance is stuck. The Web Tools Switch Admin displays the control device state and last update time (see [Figure 99](#) on page 220). You can click **Refresh** to get most recent update.

You can manually reset allegiance to bring the control device back to the neutral state by clicking **Reset Allegiance** in the FICON CUP Busy Error display (see [Figure 100](#)).

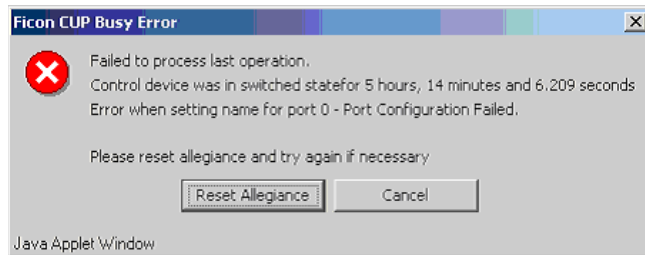


FIGURE 100 FICON CUP busy error

The following switch parameters being read or modified can cause the FICON CUP Busy error:

- Mode Register
- Port Names (also called Port Address Name)
- PDCM and Port Connectivity Attributes
- Switch enable/disable
- Switch name change

To display the control device state

1. Click a FICON-enabled switch from the [Fabric Tree](#).
2. Open the Switch Administration window as described on [page 31](#).
3. Click the **FICON CUP** tab.

The FICON CUP tabbed page displays, with the FICON Management Server subtabbed page in front (see [Figure 99](#) on page 220). All attributes on this tab are read-only until FMS Mode is enabled.

The control device state is displayed as neutral or switched in the Control Device Allegiance field.

If FMS mode is enabled, and the control device state is unavailable, the FICON CUP Busy Error is displayed. Click **Reset Allegiance** in the error message to reset the control device state to its correct state (see [Figure 100](#)).

Configuring CUP port connectivity

In the Port Connectivity subpanel (shown in [Figure 101](#) on page 226), you can manage the configuration files and active configuration. All CUP configuration files and the active configuration are listed in a table. The active configuration is listed as “Active Configuration*” and the description in the table is “Current active configuration on switch.” The other special configuration file is the IPL. Any other files displayed are user-defined configurations and are stored on the switch.

You can create, activate, copy, or delete saved CUP port connectivity configurations; however, you can only edit or copy a configuration while it is active. You can also activate, edit, or copy the IPL configuration. You must have FMS mode enabled before you can make any changes to the configurations. Click **Refresh** to get the latest configuration file list from the switch.

When creating a new configuration or editing an existing configuration, keep in mind that Web Tools port name input is restricted to printable ASCII characters. Therefore, when Web Tools displays a port name, if there are characters beyond printable ASCII characters (which would have been created by the Host Program), those characters are displayed as dots (.).

When initially installed, a switch allows any port to dynamically communicate with any other port. Two connectivity attributes are defined to restrict this any-to-any capability for external ports: *Block* and *Prohibit*.

Block is a port connectivity attribute that prevents all communication through a port. Prohibit is the port connectivity attribute that prohibits or allows dynamic communication between ports when a port is not blocked. Each port has a vector specifying its Prohibit attribute with respect to each of the other ports in the switch. This attribute is always set symmetrically in that a pair of ports is either prohibited or allowed to communicate dynamically.

The Port Connectivity table (shown in [Figure 102](#) on page 227) displays the Port number (in physical-location format), Port Name (port address name), Block attribute, Prohibit attribute, and Area Id (port address, displayed in hexadecimal) in fixed columns. The right side is a port matrix, which lists all ports by Area ID and identifies prohibited ports. Those columns are scrollable and swappable.

DISPLAYING CUP PORT CONNECTIVITY CONFIGURATIONS

Use the following procedure to display a list of CUP port connectivity configurations, as shown in [Figure 101](#) on page 226.

To display the CUP Port Connectivity Configurations list

1. Click a FICON-enabled switch from the [Fabric Tree](#).
2. Open the Switch Administration window as described on [page 31](#).
3. Click the **FICON CUP** tab.

The FICON CUP tabbed page displays, with the FICON Management Server subtabbed page in front (see [Figure 99](#) on page 220). All attributes on this page are read-only until FMS mode is enabled.

- Click the **CUP Port Connectivity** subtab (see [Figure 101](#)).

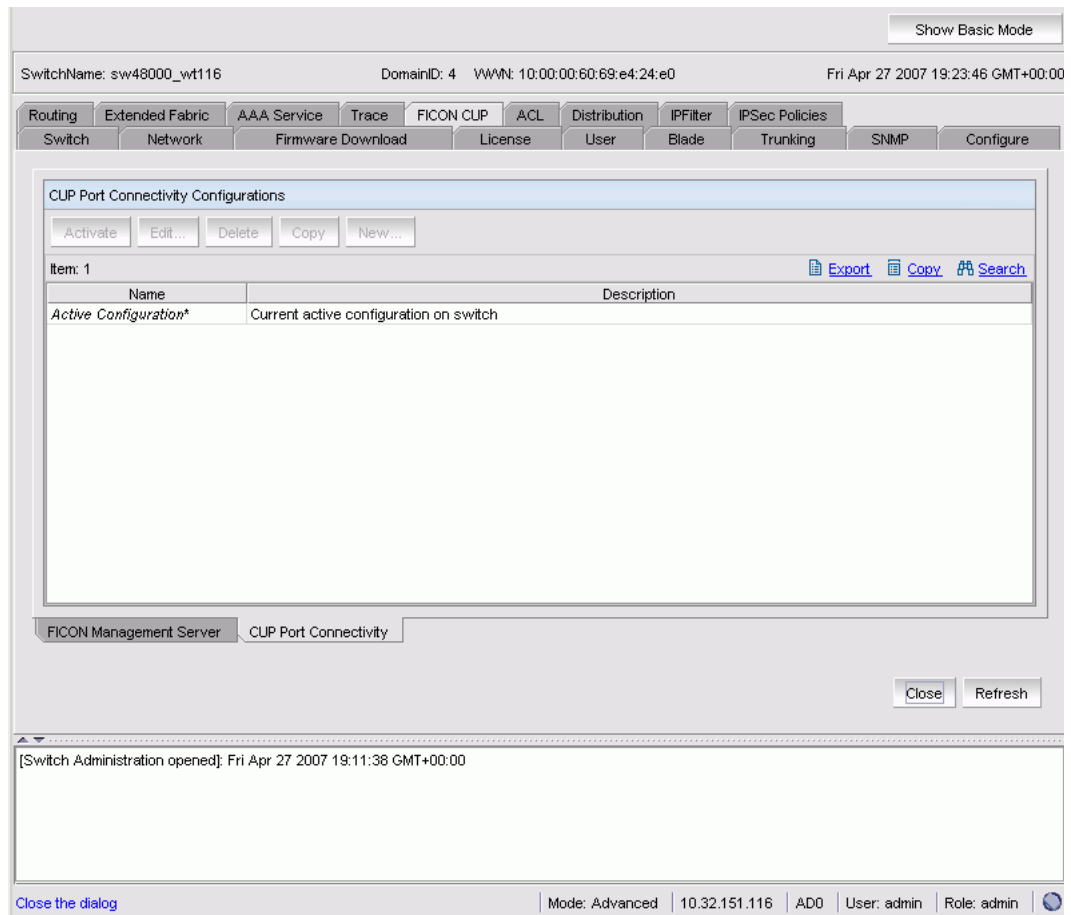


FIGURE 101 Configuring CUP port connectivity

CREATING OR EDITING CUP PORT CONNECTIVITY CONFIGURATIONS

Use the following procedure to create a new CUP port connectivity configuration or to edit an existing configuration.

To create or edit CUP port connectivity configurations

- Display the CUP port connectivity configuration list, as described on [page 225](#).
- You can either create a new configuration or edit an existing configuration.
 - To create a new configuration, click **New**.
The Create Port CUP Connectivity Configuration dialog box displays all ports and port names on the selected switch (similar to the dialog box shown in [Figure 102](#)). The Block column, Prohibit column, and prohibited ports matrix are displayed as empty, for you to configure.
 - To edit an existing configuration, click the configuration and then click **Edit**.
The Edit Port CUP Connectivity Configuration dialog box displays the content of the selected configuration from the switch in a table format (see [Figure 102](#)).

3. *Optional:* Select the check box corresponding to a port you want to block on the Block column. Repeat this step for all ports you want to block. Select the Block All check box to block all ports.
4. *Optional:* Select the check box corresponding to a port you want to prohibit on the Prohibit column. Repeat this step for all ports you want to prohibit. Select the Prohibit All check box to prohibit all ports.

The cells in the matrix are updated with “X” icons to identify prohibited ports.

5. *Optional:* Click the individual cells corresponding to the combination of ports you want to prohibit. You cannot prohibit a port to itself.
6. Review your changes. A blue background in a cell indicates that its value has been modified.
7. After you have finished making changes, do any of the following:
 - Click **Activate** to save the changes and make the configuration active immediately, as described in “[Activating a CUP Port Connectivity Configuration](#)” on page 228.
 - Click **Save** to save the changes but not make the configuration active.
 - Click **Save As** to save the configuration to a new configuration file. When you click Save As, a dialog box displays in which you should type a file name and description for the configuration file.
 - Click **Refresh** to refresh the information from the switch.
 - Click **Cancel** to cancel all changes without saving.

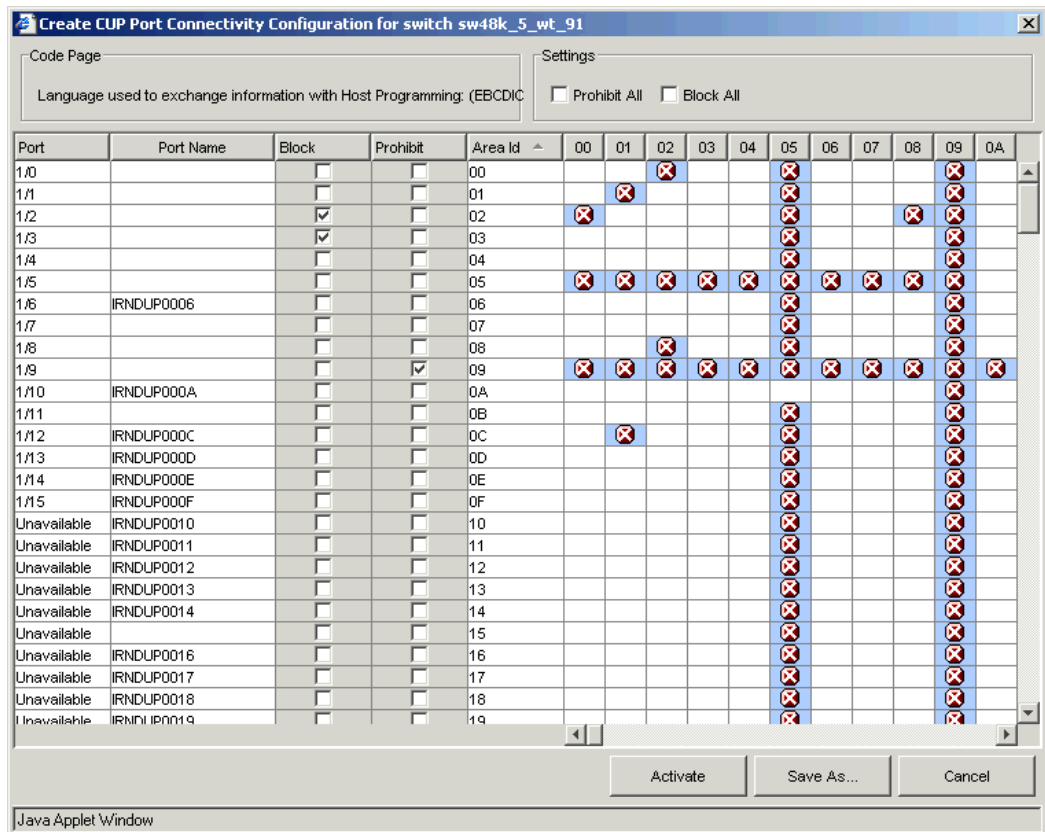


FIGURE 102 Port CUP Connectivity Configuration dialog box

ACTIVATING A CUP PORT CONNECTIVITY CONFIGURATION

When you activate a saved CUP port connectivity configuration on the switch, the preceding configuration (currently activated) is overwritten.

To activate a saved CUP port connectivity configuration

1. Open the CUP port connectivity configuration list, as described on [page 225](#).
2. Click the saved configuration from the list.
3. Click **Activate**.

The Activate CUP Port Connectivity Configuration confirmation dialog box opens.

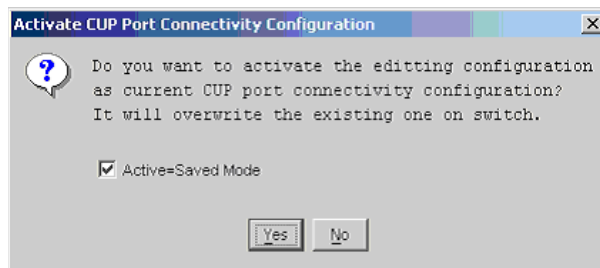


FIGURE 103 Activate CUP Port Connectivity Configuration confirmation dialog box

The message reminds you that the current configuration will be overwritten upon activation.

4. *Optional:* Click Active=Saved Mode to enable (selected) or disable (not selected) the Active=Saved FMS parameter after the configuration is activated.
5. Click **Yes** to activate the configuration or click **No** to cancel the activation.

COPYING A CUP PORT CONNECTIVITY CONFIGURATION

Use the following procedure to copy a CUP port connectivity configuration to a new configuration.

To copy a saved CUP port connectivity configuration

1. Display the CUP port connectivity configuration list, as described on [page 225](#).
2. Click a saved configuration or the active configuration from the list.
3. Click **Copy**.

The Copy CUP Port Connectivity Configuration dialog box displays.

4. In the dialog box, type a name and description for the new configuration and click **OK** to save the configuration to the target file; click **Cancel** to cancel copying the configuration.

The file name must be in alphanumeric characters and can contain only dashes or underscores as special characters.

DELETING A CUP PORT CONNECTIVITY CONFIGURATION

Use the following procedure to delete a saved CUP port connectivity configuration.

To delete a saved CUP port connectivity configuration

1. Display the CUP port connectivity configuration list, as described on [page 225](#).
2. Click the saved configuration from the list.
3. Click **Delete**.

The Delete CUP Port Connectivity Configuration confirmation dialog box displays.

4. Click **Yes** to delete the selected configuration; click **No** to cancel the deletion.

Limitations

In this chapter

This section provides the following information:

- [General Web Tools limitations](#) 231
- [Platform-specific limitations.](#) 235

General Web Tools limitations

[Table 14](#) lists general Web Tools limitations that apply to all browsers and switch platforms.

TABLE 14 Web Tools limitations

Area	Details
Blade Failure	If a blade fails on the switch, the Web Tools interface can still display slot and ports as healthy. In this case, the failure might not be visible in Web Tools until the Web Tools window is reopened.
Browser	For Internet Explore 7.0, the default setting is to disable telnet functionality. You must make the appropriate changes in the registry to enable telnet functionality if you want to use it.
Browser	Fabric Watch, Switch Admin, HA, Name Server, and Zone Admin are separate applets embedded in HTML pages. The successful launch of the applet depends on whether the browser can successfully load the HTML page. Very occasionally, you will see a blank browser window with the message “loading pages...” that is stuck. This is likely caused by a sudden loss of switch Web server (either by normal HA failover, reboot, or other causes). Workaround: If Fabric Watch, Switch Admin, HA, Name Server, or Zone Admin hang, close this window and relaunch the module.
Browser	A Web Tools browser window might stop responding following an HA failover immediately after a zoning configuration was enabled or disabled. It is likely that the Web daemon was terminated by the HA failover before the HTTP request was sent back. Workaround: If one of the Web Tools modules is hanging, close the window and relaunch the module. If the module is locked, shut down and relaunch the Web Tools application.
Browser	When you launch Fabric Watch, Switch Admin, Name Server, and Topology from Switch Explorer via Internet Explorer, the applet windows cannot be resized and the Maximize button is disabled.
Configuration	Web Tools does not support NAT router configurations and will not function correctly with switches behind a NAT router.

TABLE 14 Web Tools limitations (Continued)

Area	Details
Firmware download	<p>There are multiple phases to firmware download and activation. When Web Tools reports that firmware download has completed successfully, this indicates that a basic sanity check, package retrieval, package unloading, and verification was successful. Web Tools forces a full package install.</p> <p>A reboot is required to activate the newly downloaded firmware. This reboot is done automatically; however, although Web Tools screens will continue to be visible during the reboot, they will not be available. Wait approximately 10 minutes to ensure that all of the application windows have been restored. If Web Tools fails to respond after 20 minutes, you might need to close all Web Tools applications windows and restart them, or to contact your system administrator for network assistance.</p> <p>The Web Tools loss of network connectivity during a failover or reboot (initiated though the firmwareDownload) varies for different configurations:</p> <p>Brocade 24000 and 48000 directors: loss of network connectivity is up to 5 minutes if the power-on self-test (POST) is disabled. If POST is enabled, the loss of network connectivity can exceed 5 minutes.</p> <p>Brocade 200E, 3250, 3850, 3900, 4012, 4016, 4018, 4020, 4024, 4100, 4900, 5000, and 7500 switches: loss of network connectivity is up to 1 minute if POST is disabled. If POST is enabled, the loss of network connectivity can exceed 1 minute.</p>
Firmware downgrade	<p>If you try to run Web Tools on a switch after downgrading the firmware, Web Tools may not open. This is due to the presence of old application cache files in Java. The workaround is to delete the application cache files using the Java Control Panel.</p>
HTTP timeout	<p>Very occasionally, you might see the following message when you try to get data from a switch or to send a request to the switch:</p> <p>Failed to get switch response. Please verify the status of your last operation and try again if necessary.</p> <p>This indicates that an HTTP request did not get a response. The request was sent to the switch, but the connection was down, probably caused by a temporary loss of the Web server on the switch. Due to the nature of an HTTP connection, Web Tools will report this error after a 90-second default timeout.</p> <p>In this case, verify the status of your last request, using telnet to check related status, or click the Refresh button from the Web Tools application you were working on to retrieve related data. If your request did not get through to the switch, resubmit it. Executing a refresh from Web Tools retrieves a copy of switch data at that moment; the data you entered can be lost if it had not already committed to the switch.</p>
Java Plug-in	<p>If you remove the certificate (not recommended) from the Java Control Panel, you must close and reopen the browser for the certificate removal to take effect.</p>
Java Plug-in	<p>If you have a Web Tools session open and you open a second session using the File > New browser menu, this results in unexpected behavior of the original Web Tools session. For example, you cannot change Admin Domains in the second session. Web Tools supports only one browser instance per JRE, and when you open another window using the File > New menu, the two windows share the same JRE environment.</p> <p>Workaround: Open two independent browser sessions.</p>

TABLE 14 Web Tools limitations (Continued)

Area	Details
Loss of Connection	<p>Occasionally, you might see the following message when you try to retrieve data from the switch or send a request to the switch:</p> <p>Switch Status Checking</p> <p>The switch is not currently accessible.</p> <p>The dialog title may vary, because it indicates which module is having the problem.</p> <p>This is caused by the loss of HTTP connection with the switch, due to a variety of possible problems. Web Tools will automatically try to regain the connection. While Web Tools is trying to regain the connection, check if your Ethernet connection is still functioning. If the problem is not with the Ethernet connection, wait for Web Tools to recover the connection and display the following message:</p> <p>You will have to resubmit your request after closing this message.</p> <p>If the temporary switch connection loss is caused by switch hot code load, or other similar operation, Switch Explorer you are currently running can be downloaded from a different firmware version than the new one. In this case the following message displays:</p> <p>Switch connection is restored. The firmware version you are running is not in sync with the version currently on switch. Close your browser and re-launch Webtools.</p> <p>You need to close Switch Explorer and relaunch Web Tools to reopen the connection.</p>
Out of Memory Errors	<p>If you are managing fabrics with more than 10 switches or more than 1000 ports, or if you are using the iSCSI Gateway module extensively, you might encounter out-of-memory errors such as the following:</p> <p>java.lang.OutOfMemoryError: Java heap space</p> <p>To avoid this problem, increase the default heap size in the Java Control Panel. See “Configuring the Java plug-in” on page 4 for instructions.</p>
Performance Monitor	<p>If the Web browser crashes or the Performance Monitor license is lost while the Performance Monitoring window is running, some of the Performance Monitor resources owned by Web Tools might not be cleaned up correctly.</p> <p>Workaround: You might need to use the CLI to manually delete these counters. For example, if you detect Web Tools owned resources (using <code>perfshoweemonitor</code>), but you have verified that no Web users are actually using them, use the <code>perfdeleemonitor</code> or <code>perfcleareemonitor</code> command to free the resources.</p>
Performance Monitor	<p>For SCSI Read, Write, or Read/Write on a LUN per Port graphs, Fabric OS 4.1.0 (and later 4.x versions) allows you to enable only two bytes or less for the LUN value mask setting. Fabric OS 3.1 (and later 3.x versions) allows up to three bytes. Web Tools displays an error message if you exceed this limit.</p> <p>Workaround: There is no workaround.</p>
Performance Monitor	<p>For Brocade 24000 and 48000 directors, while monitoring the performance, if one or all the blades turn Faulty or if they are powered off or on, then the behavior of various monitoring graphs is as follows:</p> <p>The Switch Aggregate and Blade Aggregate graphs will freeze without any updates (about the traffic).</p> <p>Workaround: Close and relaunch the graphs.</p> <p>The Switch Throughput Utilization, Switch Percent Utilization, and Port Snapshot Error graphs will show the faulty/powered off slot node in the Y-Axis of the graph.</p> <p>Workaround: Launch any port selection dialog and load the graphs accordingly.</p>
Refresh option in browsers	<p>When a pop-up window requesting a user response is pushed into the background and a refresh is requested, a fatal Internet Explorer error might occur.</p> <p>Workaround: Restart the browser.</p>

TABLE 14 Web Tools limitations (Continued)

Area	Details
Refresh option in browsers	<p>Web Tools must be restarted when the Ethernet IP address is changed using the NetworkConfig View command. Web Tools appears to hang if it is not restarted after this operation is executed.</p> <p>Workaround: Restart the browser.</p>
Refresh option in browsers	<p>If you change the switch name or domain ID using the CLI after the Web Tools Switch Administration window has started, the new switch name or domain ID will not be updated on the header of the Switch Admin page. Clicking the Refresh button will not fix the problem.</p> <p>Workaround: Click the Switch tab and the Switch Admin header will update.</p>
Refresh option in browsers	<p>If you change the switch name using the Web Tools Switch Admin page or SNMP and then open a telnet window to verify the name change, the CLI prompt (for example, switch:admin>) displays the previous name. The telnet prompt cannot pick up the new switch name until the switch is fastbooted.</p> <p>Workaround: In order to display the correct switch name in the CLI prompt after a switch name update using Web Tools or SNMP, fastboot the switch.</p>
Refresh option in browsers	<p>Following a switch enable or disable, you must wait at least 25–30 seconds for the fabric to reconfigure and for FSPF route calculations to complete before requesting routing information. If accessed too early, routing information will not be shown.</p> <p>Workaround: Following a switch enable or disable, wait at least 25–30 seconds before further action.</p>
Refresh option in browsers	<p>The Web Tools Switch Explorer might continue to display a switch from the Switch View, even when the switch has been removed from the fabric.</p> <p>Workaround: If this behavior is seen, relaunch Switch Explorer. If the switch was removed from the fabric, the Fabric View window will list the switch as unavailable.</p>
Refresh option in browsers	<p>In the Switch Administration window, Switch tab, if you click the Refresh button, you might not be able to click the data entry fields to enter text. This behavior occasionally happens on a notebook or laptop computer; it rarely happens on a desktop computer.</p> <p>Workaround: If this happens, you should close the browser window and restart it.</p>
Switch Explorer closure	<p>If a session times out or you log out or close Switch Explorer window, all other windows belonging to the session are invalidated. After a short delay these windows become unusable, but are not closed automatically. You must manually close these windows.</p>
Switch View	<p>Occasionally, switches might display the port icons correctly, but be missing one or more control button icons.</p> <p>Workaround: Close the Switch View of the switch and reopen it.</p>
Windows Operating Systems	<p>Occasionally, you will not see the “Lost connection to the switch” message on the Switch View, even though the Ethernet connection has been lost. You might still be able to invoke various features from Switch View, such as Status, Fan Temp, Power, and Beacon. This problem might be seen in the Brocade 24000, for example, when you see the “Lost connection to the switch” error for a single switch in the chassis, when a lost connection affects both logical switches.</p> <p>Workaround: Verify Ethernet connection to the switch by pinging the logical switch IP address.</p>
Windows Operating Systems	<p>While working on Internet Explorer 6.0, when the user launches Switch Explorer it initially does not activate. You will have to click the window once with the mouse, press the ESC key, the Space Bar, or Enter to activate the window. This is applicable in all applets launched using IE 6.0.</p> <p>Workaround: This is not seen while working on Firefox.</p>

Platform-specific limitations

Table 15 lists Web Tools limitations that are specific to the Brocade 24000 director when it is configured to have two domains.

TABLE 15 Platform-specific limitations

Area	Details
Switch View	Neither CP is updated in the Switch View when switch 0 is being rebooted. The CP data displayed on this Switch View is dependent on switch 0, and that data is not available when switch 0 is rebooting. Workaround: Wait until the reboot is finished and Switch View polling occurs; then, the CPs will be updated properly.
Java Plug-in	The Java Plug-in might sometimes have problems focusing on a particular field in an open applet if you have the same window open for both logical switches. Workaround: When this problem occurs, close and relaunch the affected applet.

Index

Numerics

2 domain/4 domain fabric licenses, 8

A

About Discovery Domains (DD), 182

Access Control List. See ACL

access control. See RBAC.

Access Gateway mode

configuration, 191

enable, 191

enable, Web Tools, 191, 192

accessing

Switch Administration window, 138

switch event report, 50

telnet window, 32

activating

CUP port connectivity configuration, 228

licenses, 44

Ports on Demand, 73

AD. See Admin Domains.

adding

Admin Domain members, 91

performance graphs to a canvas, 133

unzoned online devices to zones, 117

WWN to zoning database, 114

zone alias members, 103

zone configuration members, 108

zone members, 105

Admin Domain window, 84

closing, 88

refreshing, 87

Admin Domains

about, 81

assigning administrators, 205

brief description, 9

creating, 88

deleting, 93

direct port membership, 64

indirect port membership, 64

modifying, 91

opening, 84

to activate/deactivate, 91

Administrative Domains. See Admin Domains

AL_PA

error graphs, creating, 132

alarm configuration report for Fabric Watch, 163

alarms, Fabric Watch

configuring, 161, 162

displaying, 163

enabling and disabling, 161

aliases, zone. See zone aliases

all access zoning, 97

arbitrated loop parameters, configuring, 42

assigning a name to a port, 70

automatic trace dump transfers, 148

B

backbone fabric, 136

backbone fabric ID, configuring, 144

backing up configuration file, 58

basic performance monitoring graphs, 127

BB credit, 40

beaconing, enabling, 55

best practices for zoning, 119

blades, enabling and disabling, 34

browsers

limitations, 231, 234

refresh frequency, setting, 3

supported, 1

buffer-limited ports, 167

C

Challenge Handshake Authentication Protocol. See CHAP

changing

chassis name, 38

domain ID, 38

passwords, 206

switch name, 37

CHAP

- authentication, 173
- secret, editing, 186
- user, creating, 186

chassis name, changing, 38

class F traffic, 40

clearing the zoning database, 116

closing

- Admin Domain window, 88
- sessions, 14
- Zone Administration window, 101

code page, displaying, 223

configuration

- Access Gateway mode, 191
- upload, 191

configuration file

- Admin Domain considerations, 58
- backing up, 58, 59
- downloading, 59
- restoring, 59
- saving, 57

configuring

- arbitrated loop parameters, 42
- backbone fabric ID, 144
- CUP port connectivity, 224
- default heap size, 4
- email notifications, 164
- ethernet IP, 32
- EX_Ports, 140
- fabric parameters, 39
- Fabric Watch thresholds, 159
- FAN frame notification parameters, 42
- FC IP address, 32
- FC ports, 67
- FCIP ports, 69
- FCR router cost, 142
- FICON Management Server parameters, 222
- FRU alarms, 162
- GigE ports for FCIP, 70
- Internet Explorer, 2
- IOD frames delivery, 199
- IP address for iSCSI Target Gateway, 177
- IP and netmask, 32
- IP interfaces for FCIP, 70
- IP route for iSCSI Target Gateway, 178
- IP routes for FCIP, 70
- Java Plug-in, 4
- link cost, 200
- long-distance settings, 169
- port speed, 67
- port type, 67, 69

ports, 63

RADIUS server, 216

routes, 197

SNMP information, 212

syslog IP address, 33

system services, 43

threshold alarms, Fabric Watch, 161

virtual channel settings, 42

Control Device state, 223

Control Unit Port. See CUP

copying CUP port connectivity configuration, 228

CP failover, initiating, 47

creating, 183

- Admin Domains, 88

- AL_PA error graphs, 132

- basic performance graphs, 127

- CHAP user for iSCSI Target Gateway, 186

- CUP port connectivity configuration, 226

- DDset, 184

- discovery domains (DD), 183

- iSCSI fibre channel zones with an effective zone configuration, 188

- iSCSI fibre channel zones with no effective zone configuration, 187

- SCC/DCC policy, 209

- SCSI command graphs, 131

- SCSI vs. IP traffic graphs, 130

- SID-DID performance graphs, 129

- user accounts, 203

- virtual targets for iSCSI Target Gateway, 179, 180

- zone aliases, 102

- zone configurations, 107

- zones, 104

CUP port connectivity configuration

- activating, 228

- copying, 228

- creating, 226

- deleting, 228

- displaying, 225

- editing, 226

customizing

- basic performance graphs, 127

- chassis name, 38

D

datafield size, 40

DDSet, creating, 184

DDSet, editing, 185

default zoning, 97

- defining device aliases, 118
- deleting
 - Admin Domains, 93
 - CUP port connectivity configuration, 228
 - user accounts, 205
 - WWN from zoning database, 115
 - zone aliases, 103
 - zone configurations, 109
 - zones, 106
- device aliases, defining, 118
- device probing, 40
- devices only view, 101
- devices only zoning, 101
- direct port membership in Admin Domains, 64
- disabling
 - automatic trace uploads, 149
 - blades, 34
 - dynamic load sharing, 199
 - Fabric Watch threshold alarms, 161
 - FICON Management Server mode, 221
 - ports, 71
 - RADIUS service, 215
 - RLS probing, 43
 - switch, 37
 - telnet access, 26
 - trunking mode, 78
 - zone configurations, 110
 - zoning, 110
- disabling an NPIV port, 72
- Discovery Domain Set. See DDSet
- Discovery Domains
 - create, 182
- displaying
 - alarms, Fabric Watch, 163
 - Control Device state, 223
 - CUP port connectivity configuration, 225
 - enabled zone configuration, 110
 - fabric events, 49
 - fan status, 150
 - FICON code page, 223
 - name server entries, 53
 - power supply status, 151
 - switch events, 50
 - switch information, 38
 - temperature status, 151
 - user account information, 203
- DLS, 199
- domain ID, changing, 38
- downloading
 - configuration file, 59
 - firmware, 60

Dynamic Load Sharing. See DLS

E

- E_D_TOV, 40
- edge fabrics
 - about, 136
- editing
 - DDset, 185
 - discovery domains (DD), 183
 - iSCSI fibre channel zone members, 187
- email notifications, 164
- enable
 - Access Gateway mode, 191, 192
- enabled zone configuration, displaying, 110
- enabling
 - automatic trace dump transfer, 149
 - beaconing, 55
 - blades, 34
 - DLS, 199
 - Fabric Watch threshold alarms, 161
 - FICON Management Server mode, 221
 - insistent domain ID mode, 41
 - iSCSI Target Gateway service, 176
 - ports, 71
 - Ports on Demand, 73
 - RADIUS service, 215
 - RLS probing, 43
 - switch, 37
 - trunking mode, 78
 - zone configurations, 109
- enabling an NPIV port, 72
- ending sessions, 14
- events
 - displaying, 49, 50
 - filtering, 51
 - severity levels, 48
- EX_Ports, configuring, 140
- exchange-based routing, 197, 199
- expiring passwords, 208
- extended fabrics, 167

F

- fabric events, 49
- fabric ID, configuring, 144
- fabric information, refreshing, 87, 99
- fabric parameters, configuring, 39

- fabric topology report, 53
- Fabric Tree, 19
- fabric view, 101
- fabric view zoning, 101
- Fabric Watch
 - about, 157
 - alarms, 161
 - thresholds, 159
- failover, initiating, 47
- FAN frame notification parameters, configuring, 42
- fan status, 150, 151
- fast boot, 39
- FC ports, configuring, 67
- FC Routing module, 138
- FC targets, searching for iSCSI Target Gateway, 181
- FC-FC routing
 - about, 135
 - setting up, 137
 - supported switches, 135
- FCIP
 - ports, configuring, 69
- FCR router cost, 142
- FCS policies configured from CLI, 26
- feature licenses, 43
- FICON Management Server
 - mode, enabling and disabling, 221
 - parameters, 222
- filtering events, 51
- Filtering IP Addresses, 34
- firmware download, 60
- FRU alarms, configuring, 162
- FSPF routing, 198
- fwdl. See firmware download.

G

- graphs for performance monitoring, 122

H

- HA. See Hi Avail
- hard zones, 95, 101
- heap size, configuring, 4
- Hi Avail
 - administering, 45
- High-Availability. See Hi Avail
- HTTP_POLICY, 25

- HTTPS protocol, 8

I

- ID_ID mode
 - about, 40
 - enabling, 41
- inactivity timeout, 12
- indirect port membership in Admin Domains, 64
- initiating CP failover, 47
- initiators for iSCSI Target Gateway, 181
- in-order delivery. See IOD
- insistent domain ID mode
 - about, 40
 - enabling, 41
- installing
 - Java Plug-in, 3, 4
 - JRE, 3
 - JRE patches on Solaris, 4
 - Solaris patches, 4
 - Web Tools license, 6
- IOD
 - configure setting, 200
 - frame delivery, 199
- IP address
 - configuring for iSCSI Target Gateway, 177
- IP address, filtering, 34
- IP and netmask, configuring, 32
- IP interfaces
 - configuring for iSCSI Target Gateway, 176
- IP interfaces, configuring for FCIP, 70
- IP routes, configuring for FCIP, 70
- IQN, 173
- iSCSI Target Gateway
 - about, 171
 - activating the service, 176
 - CHAP authentication, 173
 - CHAP secrets, editing, 186
 - CHAP user, creating, 186
 - CHAP, about, 186
 - clear all, 174
 - configure IP route, 178
 - configure the IP interface, 176
 - creating virtual targets, 179, 180
 - DDSet, creating, 184
 - DDSet, editing, 185
 - Discover Domain Set, 173
 - Discovery Domain, 173
 - discovery domain sets (DDSet), about, 184

- discovery domains (DD), 182
- discovery domains (DD), about, 182
- discovery domains, creating, 183
- discovery domains, editing, 183
- editing an iSCSI target, 181
- enabling, 176
- FC LUN, 173
- FC virtual initiator, 173
- GbE, 173
- IQN, 173
- iSCSI fibre channel zone members, editing, 187
- iSCSI fibre channel zone, creating, 187
- iSCSI fibre channel zone, creating with an effective zone configuration, 188
- iSCSI fibre channel zone, creating with no effective zone configuration, 187
- iSCSI initiator, 173
- iSCSI initiators, 181
- iSCSI Port, 173
- iSCSI session, 173
- iSCSI virtual target, 173
- launching module, 175
- LUN mapping, 173
- managing/troubleshooting accessibility, 189
- PDU, 173
- search for FC target, 181
- supported switches, 171
- VT LUN, 173
- iSCSI target, editing for iSCSI Target Gateway, 181
- ISL trunking, 77

J

- Java Plug-ins
 - configuring, 4
 - installing, 3, 4
 - supported, 2
- JRE, installing, 3

L

- launching
 - FC Routing module, 138
 - iSCSI Target Gateway module, 175
 - Web Tools, 8
- LEDs, port, 154
- license ID, displaying, 38
- license key, 6
- licenseAdd command, 6

- licensed features, 43
- licenses
 - activating, 44
 - installing Web Tools, 6
 - removing, 45
- licenseShow command, 6
- limitations
 - browsers, 231, 234
 - firmware download, 232
 - HTTP, 232, 233
 - Java, 235
 - Microsoft Windows Operating System, 234
 - Performance Monitor, 233
 - Switch View, 234, 235
- limited switch license, 8
- link cost, 200
- logging out, 14
- long-distance connection, configuring, 169
- LSAN
 - devices, 143
 - fabrics, managing, 139
 - zones, managing, 142

M

- managing RADIUS server, 213
- message severity levels, 48
- MetaSAN, 136
- modifying
 - Admin Domains, 91
 - performance graphs, 134
 - RADIUS server, 216
 - RADIUS server order, 217
 - zone aliases, 103
 - zone configurations, 108
 - zones, 105
- monitoring performance, 121
- mouse over information, 22

N

- name server entries, displaying, 53
- naming ports, 70
- netmask and IP, configuring, 32
- no access zoning, 97
- NPIV
 - about, 72
 - ports, disabling, 72

ports, enabling, 72

O

opening

in secure mode, 25

Performance Monitoring window, 126

Switch Administration window, 31

P

passwords

changing, 206

expiring, 208

rules, 207

unlocking, 208

PDU, 173

performance graphs

adding to a canvas, 133

modifying, 134

printing, 133

types of, 122

Performance Monitoring window, 126

per-frame routing priority, 40

persistently disable a port, 71

physically locating switch using beaconing, 55

PID format, 40

platforms, supported, 2

platform-specific limitations, 235

polling rates, 24

Port Administration window, 63

port membership in Admin Domains, 64

port menu, 23

port names, assigning, 70

port speed, configuring, 67

port swapping, 76

port type, configuring, 67, 69

port-based routing, 197

ports

buffer-limited, 167

configuring, 63

disabling, 71

enabling, 71

LEDs, 154

long distance parameter, 169

naming, 70

Ports on Demand, enabling, 73

power supply status, 151, 152, 153

primary FCS functionality, 26

printing

effective zone configuration, 112

fabric topology report, 53

performance graphs, 133

switch report, 38

zone configuration summary, 112

R

R_A_TOV, 40

RADIUS server

about, 213

configuring, 216

enabling and disabling, 215

modifying, 216

modifying server order, 217

removing, 217

RAM requirements, 2

RBAC

pre-defined roles, 11

rebooting the switch, 39

recommendations

configuration tasks, 27

for Web Tools, 26

for zoning, 119

mixed fabric, 26

refresh frequency, setting, 3

refresh rates, 24

refreshing

Admin Domain window, 87

fabric information, 87, 99

Switch Administration window, 31

Zone Administration window, 99

removing

Admin Domains members, 91

licenses, 45

offline devices from zoning database, 118

RADIUS server, 217

zone alias members, 103

zone configuration members, 108

zone members, 105

renaming

zone aliases, 103

zone configurations, 108

zones, 105

replacing

offline devices in zones, 118

WWN in zoning database, 115

requirements, Web Tools, 1

- restoring configuration file, 59
- right-click menu, 23
- RLS probing
 - enabling and disabling, 43
- Role-Based Access Control. See RBAC
- router cost path, 142
- routes, configuring, 197

S

- saving
 - performance graphs, 132
 - zoning changes, 87, 100
- SCC/DCC policy
 - activate, 210
 - create, 209
 - deactivate, 211
 - delete, 210
 - distribute, 211
 - edit, 210
- SCSI command graph, 131
- SCSI vs. IP traffic graph, 130
- searching zone member selection lists, 115
- secure mode, 25
- sequence level switching, 40
- session management, 12
- sessions, ending, 14
- setting
 - refresh frequency, 3
 - SNMP trap levels, 211
- severity levels, 48
- SID-DID performance graph, 129
- SNMP information, configuring, 212
- SNMP trap levels, 211
- soft zones, 95
- Solaris patches, installing, 4
- starting Web Tools, 8
- swapping port index IDs, 76
- switch
 - changing the name of, 37
 - enabling and disabling, 37
 - mouse over information, 22
 - rebooting, 39
- Switch Administration window, 29
 - opening, 31
 - refreshing, 31
- Switch Events and Switch Information, 22
- switch events, displaying, 50
- Switch Explorer
 - Admin Domains, 20
 - switch information, displaying, 38
 - switch name, changing, 37
 - switch PID format, 40
 - switch report, 38
 - switch status report, 153
 - Switch View, 21
 - Switch View buttons, 21
 - syslog IP address
 - configuring, 33
 - removing, 33
 - system services, configuring, 43

T

- telnet access disabled, 26
- telnet, install Web Tools, 6
- temperature status, 151
- threshold alarms, Fabric Watch
 - configuring threshold alarms, 161
 - enabling and disabling, 161
- timeout, session, 12
- topology report, 53
- trace dumps, 147
- troubleshooting
 - iSCSI Target Gateway, 189
 - Web Tools, 26
- trunk groups, viewing, 78
- trunking mode, enabling and disabling, 78

U

- unlocking passwords, 208
- user accounts, managing, 201

V

- value line licenses, 8
- VC Priority, 42
- viewing
 - EX_Ports, 140
 - LSAN devices, 143
 - LSAN fabrics, 139
 - LSAN zones, 142
 - swapped ports, 76
 - Switch Explorer, 17

- switch report, 38
- switch status, 152
- switches in the fabric, 25
- trunk groups, 78
- Viewing and configuring FCR router port costs, 142
- viewing FCR router cost, 142
- virtual channel settings, configuring, 42
- virtual targets, creating for iSCSI Target Gateway, 179, 180

W

Web Tools

- Access Gateway mode, enable, 191

- Web Tools, launching, 8

WWN

- adding to zones, 114
- removing from zones, 115
- replacing in zones, 115

Z

Zone Admin module

- saving changes, 87

Zone Administration window

- about, 97
- closing, 101
- refreshing, 99
- saving changes, 100

zone aliases

- adding unzoned online devices, 117
- creating, 102
- defining device aliases, 118
- deleting, 103
- description, 102
- modifying, 103
- renaming, 103
- replacing offline devices, 118

zone configurations

- analysis report, 113
- creating, 107
- deleting, 109
- disabling, 110
- enabling, 109
- example, 107
- modifying, 108
- renaming, 108
- summary report, 112

- zone member selection lists, searching, 115

zones

- about, 95
- adding unzoned online devices, 117
- adding WWNs, 114
- best practices, 119
- creating, 104
- deleting, 106
- description, 104
- enforcement, 95
- initiator/target accessibility matrix, 113
- LSAN, 142
- modifying, 105
- removing WWNs, 115
- renaming, 105
- replacing offline devices, 118
- replacing WWNs, 115
- selecting a view, 102

zoning

- all access, 97
- default zoning, 97
- no access, 97

zoning database

- clearing, 116
- managing, 114
- maximum size, 100, 110
- removing offline devices, 118

- zoning views, 101

- zoning, disabling, 110

- zoning, saving changes, 87, 100